Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/JP05/005253

International filing date: 23 March 2005 (23.03.2005)

Document type: Certified copy of priority document

Document details: Country/Office: JP
Number: 2004-085364
Filing date: 23 March 2004 (23.03.2004)

Date of receipt at the International Bureau: 12 May 2005 (12.05.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日 Date of Application:	２００４年　３月２３日
出 願 番 号 Application Number:	特願２００４－０８５３６４
パリ条約による外国への出願に用いる優先権の主張の基礎となる出願の国コードと出願番号 The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is	ＪＰ２００４－０８５３６４
出 願 人 Applicant(s):	松下電器産業株式会社

２００５年　４月２０日

特許庁長官
Commissioner,
Japan Patent Office

小 川

【書類名】　特許願
【整理番号】　2048160094
【提出日】　平成16年 3月23日
【あて先】　特許庁長官　殿
【国際特許分類】　G09C　1/00
【発明者】
　【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
　【氏名】　井藤　好克
【発明者】
　【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
　【氏名】　宮▲ざき▼　雅也
【発明者】
　【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
　【氏名】　大森　基司
【発明者】
　【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
　【氏名】　原田　俊治
【発明者】
　【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
　【氏名】　横田　薫
【発明者】
　【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
　【氏名】　中野　稔久
【発明者】
　【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
　【氏名】　▲たか▼橋　潤
【特許出願人】
　【識別番号】　000005821
　【氏名又は名称】　松下電器産業株式会社
【代理人】
　【識別番号】　100090446
　【弁理士】
　【氏名又は名称】　中島　司朗
【手数料の表示】
　【予納台帳番号】　014823
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　特許請求の範囲　1
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1
　【包括委任状番号】　9003742

【書類名】特許請求の範囲
【請求項１】
コンテンツを保持する端末装置から、可搬媒体へコンテンツを移動可能な著作権保護システムであって、
前記端末装置は、第１のコンテンツを記憶する記憶部を備え、
前記第１のコンテンツを前記可搬媒体に移動する際、前記第１のコンテンツの一部である部分情報を消去して、前記第１のコンテンツを利用不可状態にして、
前記可搬媒体は、第２のコンテンツを記録するコンテンツ記録領域を備え、
前記移動するコンテンツを前記コンテンツ記録領域に記録することを特徴とする著作権保護システム。
【請求項２】
前記著作権保護システムであって、
前記可搬媒体は、前記部分情報を記録する部分情報記録領域を備え、
前記端末装置は、前記端末装置から前記可搬媒体へコンテンツを移動する際に、前記第１のコンテンツから前記部分情報を消去するに先立ち、前記部分情報を前記部分情報記録領域に記録することを特徴とする請求項１記載の著作権保護システム。
【請求項３】
前記著作権保護システムであって、
前記端末装置は、前記端末装置から前記可搬媒体へ移動したコンテンツを再度前記端末装置へ戻す際に、
前記部分情報記録領域に記録した部分情報を前記第１のコンテンツに書き戻して利用可能状態にすることを特徴とする請求項２記載の著作権保護システム。
【請求項４】
前記著作権保護システムであって、
前記端末装置の記憶部は、第１のコンテンツを１つ以上のブロックに分割して記録し、
前記部分情報は、前記ブロックから各々選択することを特徴とする請求項１から請求項３のいずれか１項に記載の著作権保護システム。
【請求項５】
前記著作権保護システムであって、
前記端末装置はコンテンツを暗号化する暗号化部と、前記暗号化部により暗号化されたコンテンツを復号する復号化部を備え、
第１のコンテンツは前記暗号化部により暗号化して前記記憶部に記憶され、
前記第１のコンテンツを前記可搬媒体に移動する際、
前記記憶部に記憶された暗号化コンテンツから前記部分情報を選択して消去して、前記第１のコンテンツを利用不可状態にすることを特徴とする請求項１から請求項４のいずれかに記載の著作権保護システム。
【請求項６】
前記著作権保護システムであって、
前記端末装置はコンテンツを暗号化する暗号化部と、前記暗号化部により暗号化されたコンテンツを復号する復号化部を備え、
第１のコンテンツは前記暗号化部により暗号化して前記記憶部に記憶され、
前記第１のコンテンツを前記可搬媒体に移動する際、
前記記憶部に記憶された暗号化コンテンツを前記復号化部で復号化したコンテンツから前記部分情報を選択し、
前記復号化したコンテンツの前記部分情報に対応する部分を消去した情報を、前記暗号化部で再度暗号化し、
前記記憶部に記憶された暗号化コンテンツを前記再度暗号化した情報で上書きすることで、前記第１のコンテンツを利用不可能状態にすることを特徴とする請求項１から請求項４のいずれか１項に記載の著作権保護システム。
【請求項７】

前記著作権保護システムであって、
前記端末装置はコンテンツを暗号化する暗号化部と、前記暗号化部により暗号化されたコンテンツを復号する復号化部を備え、
第１のコンテンツは前記暗号化部により暗号化して前記記憶部に記憶され、
前記第１のコンテンツを前記可搬媒体に移動する際、
前記記憶部に記憶された暗号化コンテンツを前記復号化部で復号化したコンテンツから前記部分情報の位置を選択し、
前記記憶部に記憶された暗号化コンテンツの、前記選択した位置に対応する部分を部分情報とし、
前記記憶部に記憶された暗号化コンテンツの、前記選択した位置に対応する部分を消去することで、前記第１のコンテンツを利用不可能状態にすることを特徴とする請求項１から請求項４のいずれか１項に記載の著作権保護システム。
【請求項８】
前記著作権保護システムであって、
前記部分情報を暗号化する部分情報暗号化部と、前記部分情報暗号化部により暗号化された部分情報を復号化する部分情報復号化部を備え、
前記部分情報を前記部分情報記録領域に記録するに際し、
前記部分情報を前記部分情報暗号化部により暗号化して記録することを特徴とする請求項２から請求項７のいずれか１項に記載の著作権保護システム。
【請求項９】
前記著作権保護システムであって、
前記部分情報を暗号化もしくは復号化する鍵は、コンテンツの暗号化に用いる鍵と同じであることを特徴とする請求項８に記載の著作権保護システム。
【請求項１０】
コンテンツを保持して、可搬媒体へコンテンツを移動可能な端末装置であって、
前記端末装置は、第１のコンテンツを記憶する記憶部を備え、
前記第１のコンテンツを前記可搬媒体に移動する際、前記第１のコンテンツの一部である部分情報を消去して、前記第１のコンテンツを利用不可状態にして、
前記可搬媒体は、第２のコンテンツを記録するコンテンツ記録領域を備え、
前記移動するコンテンツを前記コンテンツ記録領域に記録することを特徴とする端末装置。
【請求項１１】
前記端末装置であって、
前記可搬媒体は、前記部分情報を記録する部分情報記録領域を備え、
前記端末装置は、前記端末装置から前記可搬媒体へコンテンツを移動する際に、前記第１のコンテンツから前記部分情報を消去するに先立ち、前記部分情報を前記部分情報記録領域に記録することを特徴とする請求項１０記載の端末装置。
【請求項１２】
前記端末装置であって、
前記端末装置は、前記端末装置から前記可搬媒体へ移動したコンテンツを再度前記端末装置へ戻す際に、
前記部分情報記録領域に記録した部分情報を前記第１のコンテンツに書き戻して利用可能状態にすることを特徴とする請求項１１記載の端末装置。
【請求項１３】
前記端末装置であって、
前記端末装置の記憶部は、第１のコンテンツを１つ以上のブロックに分割して記録し、
前記部分情報は、前記ブロックから各々選択することを特徴とする請求項１０から請求項１２のいずれか１項に記載の端末装置。
【請求項１４】
前記端末装置であって、

前記端末装置はコンテンツを暗号化する暗号化部と、前記暗号化部により暗号化されたコンテンツを復号する復号化部を備え、
第１のコンテンツは前記暗号化部により暗号化して前記記憶部に記憶され、
前記第１のコンテンツを前記可搬媒体に移動する際、
前記記憶部に記憶された暗号化コンテンツから前記部分情報を選択して消去して、前記第１のコンテンツを利用不可状態にすることを特徴とする請求項１０から請求項１３のいずれか１項に記載の端末装置。
【請求項１５】
前記端末装置であって、
前記端末装置はコンテンツを暗号化する暗号化部と、前記暗号化部により暗号化されたコンテンツを復号する復号化部を備え、
第１のコンテンツは前記暗号化部により暗号化して前記記憶部に記憶され、
前記第１のコンテンツを前記可搬媒体に移動する際、
前記記憶部に記憶された暗号化コンテンツを前記復号化部で復号化したコンテンツから前記部分情報を選択し、
前記復号化したコンテンツの前記部分情報に対応する部分を消去した情報を、前記暗号化部で再度暗号化し、
前記記憶部に記憶された暗号化コンテンツを前記再度暗号化した情報で上書きすることで、前記第１のコンテンツを利用不可能状態にすることを特徴とする請求項１０から請求項１３のいずれか１項に記載の端末装置。
【請求項１６】
前記端末装置であって、
前記端末装置はコンテンツを暗号化する暗号化部と、前記暗号化部により暗号化されたコンテンツを復号する復号化部を備え、
第１のコンテンツは前記暗号化部により暗号化して前記記憶部に記憶され、
前記第１のコンテンツを前記可搬媒体に移動する際、
前記記憶部に記憶された暗号化コンテンツを前記復号化部で復号化したコンテンツから前記部分情報の位置を選択し、
前記記憶部に記憶された暗号化コンテンツの、前記選択した位置に対応する部分を部分情報とし、
前記記憶部に記憶された暗号化コンテンツの、前記選択した位置に対応する部分を消去することで、前記第１のコンテンツを利用不可能状態にすることを特徴とする請求項１０から請求項１３のいずれか１項に記載の端末装置。
【請求項１７】
前記端末装置であって、
前記部分情報を暗号化する部分情報暗号化部と、前記部分情報暗号化部により暗号化された部分情報を復号化する部分情報復号化部を備え、
前記部分情報を前記部分情報記録領域に記録するに際し、
前記部分情報を前記部分情報暗号化部により暗号化して記録することを特徴とする請求項１１から請求項１６のいずれか１項に記載の端末装置。
【請求項１８】
前記端末装置であって、
前記部分情報を暗号化もしくは復号化する鍵は、コンテンツの暗号化に用いる鍵と同じであることを特徴とする請求項１７に記載の端末装置。

【書類名】明細書
【発明の名称】記録再生装置、可搬媒体、及び著作権保護システム
【技術分野】
【０００１】
本発明は、コンテンツの不正利用防止を目的とした記録再生装置、及び可搬媒体を含む著作権保護システムに関し、特に、不正利用を防止しつつユーザの利便性を高める技術に関する。
【背景技術】
【０００２】
近年、ＢＳデジタル放送や地上デジタル放送の開始に伴い、映画等のデジタルコンテンツが広く配信されるようになってきている。デジタルコンテンツ（以下、コンテンツ）は複製が容易であるため、インターネットやその他の媒体を介した海賊行為、並びに複製コンテンツの再配信などの不正行為に対する懸念が高まっており、これら不正行為に対抗（コンテンツを保護）するための技術開発が進められている。
【０００３】
このようなコンテンツの保護技術に関する規格として、例えば、ＤＴＣＰ（Ｄｉｇｉｔａｌ　Ｔｒａｎｓｍｉｓｓｉｏｎ　Ｃｏｎｔｅｎｔ　Ｐｒｏｔｅｃｔｉｏｎ）がある。ＤＴＣＰは、コンテンツをデジタル転送する際に、コンテンツを暗号化するなどして不正コピーを防止する技術である。ＤＴＣＰのようなコンテンツ保護技術においては、コンテンツに、「Ｃｏｐｙ　Ｎｏ　Ｍｏｒｅ」、「Ｃｏｐｙ　Ｏｎｅ　Ｇｅｎｅｒａｔｉｏｎ」等のコピー制御情報（ＣＣＩ：Ｃｏｐｙ　Ｃｏｎｔｒｏｌ　Ｉｎｆｏｒｍａｔｉｏｎ）を付与する。「Ｃｏｐｙ　Ｎｏ　Ｍｏｒｅ」はコンテンツのコピーが禁止されていることを表し、「Ｃｏｐｙ　Ｏｎｅ　Ｇｅｎｅｒａｔｉｏｎ」はコンテンツのコピーが１回だけ許されていることを表す。従って、コピー制御情報として「Ｃｏｐｙ　Ｏｎｅ　Ｇｅｎｅｒａｔｉｏｎ」が付与されたコンテンツをコピーすると、コピーによって新たに得られたコンテンツには、コピー制御情報として「Ｃｏｐｙ　Ｎｏ　Ｍｏｒｅ」が付与される。
【０００４】
一方で、コピー制御情報として「Ｃｏｐｙ　Ｎｏ　Ｍｏｒｅ」が付与されたコンテンツであっても、他の記録媒体、あるいは他の装置へ移動させたいという要望がある。例えば、デジタルテレビに内蔵されているＨＤＤ（Ｈａｒｄ　Ｄｉｓｋ　Ｄｒｉｖｅ）に記録されているコンテンツをＤＶＤ－ＲＡＭに移動させて保存版として保管しておきたいような場合である。この際（ＨＤＤからＤＶＤ－ＲＡＭにコンテンツを移動させた場合）、デジタルテレビ内蔵ＨＤＤの当該コンテンツは、当然、再生できない状態にされなければならない。例えば、内蔵ＨＤＤからＤＶＤ－ＲＡＭにコンテンツをコピーした後に、内蔵ＨＤＤに記録されているコンテンツを消去するなどしてコンテンツを無効化する、すなわちコンテンツを利用できない状態にする方法などが考えられる。しかしながら、コンテンツの移動に先立ってデジタルテレビから内蔵ＨＤＤを取り出し、これをパーソナルコンピュータに接続してバックアップを作成し、コンテンツを移動した後にバックアップしておいたデータを内蔵ＨＤＤに戻すという操作が行われると、コンテンツを何度でも移動できることになり、事実上不正コピーを防止することができなくなる。
【０００５】
また、コンテンツの移動中に電源断などの原因により、移動元と移動先のコンテンツが共に損なわれ、コンテンツとして利用できなくなることは、コンテンツを利用するユーザにとっては不便である。さらに、このようにして利用できなくなったコンテンツを再度入手するために出費が必要な場合には経済的な損失も発生する。
上記課題を解決するための従来技術として、不正コピーを防止しながら、コンテンツの喪失を招くことなく、コンテンツの移動を可能にする技術が特許文献１に開示されている。
【特許文献１】特開２００３－２２８５２２号公報
【非特許文献１】「現代暗号理論」、池野信一、小山謙二、電子通信学会

【非特許文献２】「暗号理論入門」、岡本栄司、共立出版株式会社
【発明の開示】
【発明が解決しようとする課題】
【０００６】
しかしながら、移動元のコンテンツが高画質コンテンツであり、コンテンツのサイズに比べて、移動先の記録容量が小さい場合には、コンテンツの移動前に、その画質を劣化させるなどしてサイズを小さく圧縮変換してから移動を行うのが通例であるが、前記構成のようにコンテンツを消去するなどして移動元のコンテンツを無効化する場合、圧縮変換された（画質の劣化した）コンテンツだけがユーザの下に残ることになる。すなわち、再び記録容量の大きな内蔵ＨＤＤへコンテンツを戻す（移動する）場合であっても、画質の劣化されたコンテンツを高画質コンテンツへ変換することは不可能であり、元々の高画質コンテンツは復元されないため、これはコンテンツを利用するユーザの利便性が損なわれることにつながる。
【０００７】
本発明は、前記課題を解決するものであって、不正コピーを防止しながら、コンテンツの喪失を招くことなくコンテンツの移動を可能にして、さらに、サイズを小さくする圧縮変換後であっても、当該コンテンツを移動元に戻す場合には、元々の高画質コンテンツの復元を可能にする記録再生装置、並びに可搬媒体を含む著作権保護システムの提供を目的とする。
【課題を解決するための手段】
【０００８】
本発明は、コンテンツを保持する端末装置から、可搬媒体へコンテンツを移動可能な著作権保護システムであって、前記端末装置は、第１のコンテンツを記憶する記憶部を備え、前記第１のコンテンツを前記可搬媒体に移動する際、前記第１のコンテンツの一部である部分情報を消去して、前記第１のコンテンツを利用不可状態にして、前記可搬媒体は、第２のコンテンツを記録するコンテンツ記録領域を備え、前記移動するコンテンツを前記コンテンツ記録領域に記録することを特徴とする。
【０００９】
また、本発明は、前記著作権保護システムであって、前記可搬媒体は、前記部分情報を記録する部分情報記録領域を備え、前記端末装置は、前記端末装置から前記可搬媒体へコンテンツを移動する際に、前記第１のコンテンツから前記部分情報を消去するに先立ち、前記部分情報を前記部分情報記録領域に記録することを特徴とする。
また、本発明は、前記著作権保護システムであって、前記端末装置は、前記端末装置から前記可搬媒体へ移動したコンテンツを再度前記端末装置へ戻す際に、前記部分情報記録領域に記録した部分情報を前記第１のコンテンツに書き戻して利用可能状態にすることを特徴とする。
【００１０】
また、本発明は、前記著作権保護システムであって、前記端末装置の記憶部は、第１のコンテンツを１つ以上のブロックに分割して記録し、前記部分情報は、前記ブロックから各々選択することを特徴とする。
また、本発明は、前記著作権保護システムであって、前記端末装置はコンテンツを暗号化する暗号化部と、前記暗号化部により暗号化されたコンテンツを復号する復号化部を備え、第１のコンテンツは前記暗号化部により暗号化して前記記憶部に記憶され、前記第１のコンテンツを前記可搬媒体に移動する際、前記記憶部に記憶された暗号化コンテンツから前記部分情報を選択して消去して、前記第１のコンテンツを利用不可状態にすることを特徴とする。
【００１１】
また、本発明は、前記著作権保護システムであって、前記端末装置はコンテンツを暗号化する暗号化部と、前記暗号化部により暗号化されたコンテンツを復号する復号化部を備え、第１のコンテンツは前記暗号化部により暗号化して前記記憶部に記憶され、前記第１

のコンテンツを前記可搬媒体に移動する際、前記記憶部に記憶された暗号化コンテンツを前記復号化部で復号化したコンテンツから前記部分情報を選択し、前記復号化したコンテンツの前記部分情報に対応する部分を消去した情報を、前記暗号化部で再度暗号化し、前記記憶部に記憶された暗号化コンテンツを前記再度暗号化した情報で上書きすることで、前記第１のコンテンツを利用不可能状態にすることを特徴とする。

【００１２】

また、本発明は、前記著作権保護システムであって、前記端末装置はコンテンツを暗号化する暗号化部と、前記暗号化部により暗号化されたコンテンツを復号する復号化部を備え、第１のコンテンツは前記暗号化部により暗号化して前記記憶部に記憶され、前記第１のコンテンツを前記可搬媒体に移動する際、前記記憶部に記憶された暗号化コンテンツを前記復号化部で復号化したコンテンツから前記部分情報の位置を選択し、前記記憶部に記憶された暗号化コンテンツの、前記選択した位置に対応する部分を部分情報とし、前記記憶部に記憶された暗号化コンテンツの、前記選択した位置に対応する部分を消去することで、前記第１のコンテンツを利用不可能状態にすることを特徴とする。

【００１３】

また、本発明は、前記著作権保護システムであって、前記部分情報を暗号化する部分情報暗号化部と、前記部分情報暗号化部により暗号化された部分情報を復号化する部分情報復号化部を備え、前記部分情報を前記部分情報記録領域に記録するに際し、前記部分情報を前記部分情報暗号化部により暗号化して記録することを特徴とする。

また、本発明は、前記著作権保護システムであって、前記部分情報を暗号化もしくは復号化する鍵は、コンテンツの暗号化に用いる鍵と同じであることを特徴とする。

【００１４】

また本発明は、コンテンツを保持する端末装置から、可搬媒体へコンテンツを移動可能な端末装置であって、前記端末装置は、第１のコンテンツを記憶する記憶部を備え、前記第１のコンテンツを前記可搬媒体に移動する際、前記第１のコンテンツの一部である部分情報を消去して、前記第１のコンテンツを利用不可状態にして、前記可搬媒体は、第２のコンテンツを記録するコンテンツ記録領域を備え、前記移動するコンテンツを前記コンテンツ記録領域に記録することを特徴とする。

【００１５】

また、本発明は、前記端末装置であって、前記可搬媒体は、前記部分情報を記録する部分情報記録領域を備え、前記端末装置は、前記端末装置から前記可搬媒体へコンテンツを移動する際に、前記第１のコンテンツから前記部分情報を消去するに先立ち、前記部分情報を前記部分情報記録領域に記録することを特徴とする。

また、本発明は、前記端末装置であって、前記端末装置は、前記端末装置から前記可搬媒体へ移動したコンテンツを再度前記端末装置へ戻す際に、前記部分情報記録領域に記録した部分情報を前記第１のコンテンツに書き戻して利用可能状態にすることを特徴とする。

【００１６】

また、本発明は、前記端末装置であって、前記端末装置の記憶部は、第１のコンテンツを１つ以上のブロックに分割して記録し、前記部分情報は、前記ブロックから各々選択することを特徴とする。

また、本発明は、前記端末装置であって、前記端末装置はコンテンツを暗号化する暗号化部と、前記暗号化部により暗号化されたコンテンツを復号する復号化部を備え、第１のコンテンツは前記暗号化部により暗号化して前記記憶部に記憶され、前記第１のコンテンツを前記可搬媒体に移動する際、前記記憶部に記憶された暗号化コンテンツから前記部分情報を選択して消去して、前記第１のコンテンツを利用不可状態にすることを特徴とする。

【００１７】

また、本発明は、前記端末装置であって、前記端末装置はコンテンツを暗号化する暗号化部と、前記暗号化部により暗号化されたコンテンツを復号する復号化部を備え、第１の

コンテンツは前記暗号化部により暗号化して前記記憶部に記憶され、前記第１のコンテンツを前記可搬媒体に移動する際、前記記憶部に記憶された暗号化コンテンツを前記復号化部で復号化したコンテンツから前記部分情報を選択し、前記復号化したコンテンツの前記部分情報に対応する部分を消去した情報を、前記暗号化部で再度暗号化し、前記記憶部に記憶された暗号化コンテンツを前記再度暗号化した情報で上書きすることで、前記第１のコンテンツを利用不可能状態にすることを特徴とする。

【００１８】

また、本発明は、前記端末装置であって、前記端末装置はコンテンツを暗号化する暗号化部と、前記暗号化部により暗号化されたコンテンツを復号する復号化部を備え、第１のコンテンツは前記暗号化部により暗号化して前記記憶部に記憶され、前記第１のコンテンツを前記可搬媒体に移動する際、前記記憶部に記憶された暗号化コンテンツを前記復号化部で復号化したコンテンツから前記部分情報の位置を選択し、前記記憶部に記憶された暗号化コンテンツの、前記選択した位置に対応する部分を部分情報とし、前記記憶部に記憶された暗号化コンテンツの、前記選択した位置に対応する部分を消去することで、前記第１のコンテンツを利用不可能状態にすることを特徴とする。

【００１９】

また、本発明は、前記端末装置であって、前記部分情報を暗号化する部分情報暗号化部と、前記部分情報暗号化部により暗号化された部分情報を復号化する部分情報復号化部を備え、前記部分情報を前記部分情報記録領域に記録するに際し、前記部分情報を前記部分情報暗号化部により暗号化して記録することを特徴とする。

また、本発明は、前記端末装置であって、前記部分情報を暗号化もしくは復号化する鍵は、コンテンツの暗号化に用いる鍵と同じであることを特徴とする。

【発明の効果】

【００２０】

本発明によれば、コンテンツの移動元の記録再生装置が、コンテンツの移動時に当該コンテンツの部分情報を移動させることにより、記録再生装置内のコンテンツをすべて消去することなく利用不可状態にし、移動したコンテンツを再び当該記録再生装置へ戻す場合には、前記部分情報を元に戻す（移動させる）ことにより、元々の高画質コンテンツを復元可能（利用可能）にすることが可能となる。

【発明を実施するための最良の形態】

【００２１】

以下、本発明の実施の形態について、図面を参照しながら説明する。図１は、本発明に係る著作権保護システムの全体構成を示すブロック図である。このシステムは、コンテンツを供給するコンテンツ供給装置１０１と、前記コンテンツを獲得して、コンテンツの記録、並びに再生を行い、さらにコンテンツの移動を実行する記録再生装置１０２と、前記移動するコンテンツを獲得する記録再生装置１０３、あるいは可搬媒体１０４からなる。

【００２２】

記録再生装置１０２は、コンテンツ供給装置１０１からコンテンツを受信して記録する際、当該コンテンツを暗号化して、例えば内蔵ＨＤＤに記録する。そして、当該コンテンツを移動する際は、移動先となる装置、あるいは可搬媒体が正規装置、あるいは正規可搬媒体であるか否かを確認（認証）した上で、コンテンツの移動を実行する。さらに、記録再生装置１０２は、コンテンツの移動が完了した後に、内部に記録するコンテンツを利用できない状態にする。ここで、認証技術は、例えばＤＴＣＰ規格で定められた手順に従う、あるいは非特許文献１、並びに非特許文献２に開示される公知の任意の技術で実現可能なため、その詳細についてはここでは言及しない。

【００２３】

（実施の形態１）

図２は、本発明の実施の形態１における、記録再生装置１０２が可搬媒体１０４にコンテンツを移動させる場合の記録再生装置１０２、並びに可搬媒体１０４の機能を示す機能ブロック図である。

記録再生装置１０２は、外部からのコンテンツを受信するコンテンツ受信部２０１と、前記受信したコンテンツを暗号化するために用いる装置記録鍵を記憶する装置記録鍵記憶部２０２と、前記装置記録鍵を用いて、前記受信したコンテンツを暗号化する暗号化部２０３と、前記暗号化したコンテンツを記録する暗号化コンテンツ記録部２０４と、暗号化コンテンツ記録部２０４に記録された前記暗号化したコンテンツを読み出す暗号化コンテンツ読出し部２０５と、前記装置記録鍵を用いて、暗号化コンテンツ読出し部２０５が読み出した前記暗号化したコンテンツを復号する復号部２０６と、前記復号したコンテンツを（圧縮）変換する変換部２０７と、変換部２０７が変換したコンテンツを暗号化するために用いる媒体記録鍵を生成する媒体記録鍵生成部２０８と、前記媒体記録鍵を記憶する媒体記録鍵記憶部２０９と、前記媒体記録鍵を用いて、変換部２０７が変換したコンテンツを暗号化する暗号化部２１０と、暗号化コンテンツ読出し部２０５が読み出した前記暗号化したコンテンツから部分情報を選択する部分情報選択部２１１と、前記部分情報を記憶する部分情報記憶部２１２と、部分情報記憶部２１２に記憶された前記部分情報に対応して暗号化コンテンツ記録部２０４に書込みを行う部分情報書込部２１３と、前記暗号化したコンテンツ、前記媒体記録鍵、並びに前記部分情報を可搬媒体１０４に書き込む、あるいは可搬媒体１０４から読み出す書込／読出部２１４とを備える。媒体記録鍵記憶部２０９に記憶する鍵データは、書込／読出部２１４を介して当該鍵データが媒体に書き込まれた後は、そのデータが消去される。

【００２４】

また、可搬媒体１０４は、暗号化コンテンツを記録する暗号化コンテンツ領域２２１と、媒体記録鍵を記録する媒体記録鍵領域２２２と、部分情報を記録する部分情報領域２２３を備える。可搬媒体１０４が備える媒体記録鍵領域２２２は、鍵を記録するための安全な領域であり、例えば、可搬媒体との認証をパスした装置のみがデータの読み書き可能となるような領域である。

【００２５】

図３は暗号化コンテンツ記録部に記録された暗号化コンテンツを示す図である。暗号化コンテンツは１つ以上のブロック（ＥＣ１［1］、ＥＣ１［2］、・・・、ＥＣ１［N］）に分けて記録され、各ブロックは装置記録鍵を用いて暗号化されている。

次に、図４および図５を用いて、記録再生装置１０２から、可搬媒体１０４へコンテンツを移動する場合の動作について説明する。

【００２６】

Ｓ４０１：記録再生装置１０２は、媒体記録鍵生成部２０８において媒体記録鍵Ｋ２を生成して、媒体記録鍵記憶部２０９に、前記生成した媒体記録鍵を記憶する。

Ｓ４０２：記録再生装置１０２は、書込／読出部２１４を介して媒体記録鍵Ｋ２を媒体記録鍵領域２２２に書き出す。

Ｓ４０３：記録再生装置１０２は、暗号化コンテンツ読出し部２０５において暗号化コンテンツ記録部２０４に記録する暗号化コンテンツの先頭ブロックＥＣ１［ｉ］（ｉ＝１）を読み出す。

【００２７】

Ｓ４０４：記録再生装置１０２は、暗号化コンテンツのブロックの読み出しに失敗したらＳ４０６に処理を分岐する。そうでなければ、Ｓ５００に処理を分岐する。

Ｓ５００：読み出した暗号化コンテンツのブロックを可搬媒体に移動する。

Ｓ４０５：記録再生装置１０２は、暗号化コンテンツ読出し部２０５において暗号化コンテンツ記録部２０４に記録する暗号化コンテンツの次ブロックＥＣ１［ｉ］（ｉ＝ｉ＋１）を読み出す。

【００２８】

Ｓ４０６：記録再生装置１０２は、媒体記録鍵記憶部２０９に記録された媒体記録鍵Ｋ２を消去する。

以下のステップは、Ｓ５００を詳細化したものである。

Ｓ５０１：記録再生装置１０２は、暗号化コンテンツの１ブロックＥＣ１［ｉ］を復号

部２０６において、装置記録鍵記憶部２０２に記憶する装置記録鍵Ｋ１を用いて復号し、Ｃ１［ｉ］を生成する。

【００２９】

Ｓ５０２：記録再生装置１０２は、変換部２０７において、Ｓ５０１で復号したブロックＣ１［ｉ］を（圧縮）変換し、Ｃ２［ｉ］を生成する。

Ｓ５０３：記録再生装置１０２は、暗号化部２１０において、Ｓ４０１で生成／記憶した媒体記録鍵Ｋ２を用いて、Ｓ５０２で変換したコンテンツＣ２［ｉ］を暗号化し、ＥＣ２［ｉ］を生成する。

【００３０】

Ｓ５０４：記録再生装置１０２は、Ｓ５０３で暗号化したコンテンツＥＣ２［ｉ］を、書込／読出部２１４を介して可搬媒体１０４の暗号化コンテンツ領域２２１へ記録する。

Ｓ５０５：記録再生装置１０２は、部分情報選択部２１１において、暗号化コンテンツの１ブロックＥＣ１［ｉ］から、部分情報ＰＥＣ１［ｉ］を選択（例えば、ブロックの先頭から５１２ｂｙｔｅを選択）し、部分情報記憶部２１２へ記録する。

【００３１】

Ｓ５０６：記録再生装置１０２は、暗号化コンテンツ記録部２０４に記録された暗号化コンテンツの、部分情報記憶部２１２へ記録されたＰＥＣ１［ｉ］に対応する部分を無意味な情報（例えば全て０）で上書きする。

Ｓ５０７：記録再生装置１０２は、部分情報記憶部２１２に記憶する部分情報ＰＥＣ１［ｉ］を、書込／読出部２１４を介して可搬媒体１０４の部分情報領域２２３へ記録する。

【００３２】

Ｓ５０８：記録再生装置１０２は装置内の、部分情報記憶部２１２に記憶する部分情報ＰＥＣ１［ｉ］と、Ｓ５０１で生成したＣ１［ｉ］と、Ｓ５０２で生成したＣ２［ｉ］と、Ｓ５０３で生成したＥＣ２［ｉ］を消去する。

図６は、記録再生装置１０２から可搬媒体１０４へのコンテンツの移動が完了したときの、可搬媒体１０４の記録状態を示した図である。

【００３３】

次に、図７を用いて、可搬媒体１０４から、記録再生装置１０２へコンテンツを移動する場合の動作について説明する。

Ｓ７０１：可搬媒体１０４は、暗号化コンテンツ領域２２１に記録する暗号化コンテンツＥＣ２［ｉ］（ｉ＝１～Ｎ）、並びに媒体記録鍵領域２２２に記録する媒体記録鍵Ｋ２を消去する。

【００３４】

Ｓ７０２：記録再生装置１０２は、可搬媒体１０４の部分情報領域２２３に記録する部分情報の先頭ブロックＰＥＣ１［ｉ］（ｉ＝１）を書込／読出部２１４を介して読み出す。

Ｓ７０３：記録再生装置１０２は、部分情報のブロックの読み出しに失敗したら処理を終了する。そうでなければ、Ｓ７０４に処理を分岐する。

【００３５】

Ｓ７０４：記録再生装置１０２は、読出した部分情報ＰＥＣ１［ｉ］を部分情報記憶部２１２へ記録する。

Ｓ７０５：記録再生装置１０２は、部分情報記憶部２１２へ記録されたＰＥＣ１［ｉ］を、暗号化コンテンツ記録部２０４に記録された暗号化コンテンツの対応する部分へ上書きする。

【００３６】

Ｓ７０６：記録再生装置１０２は、部分情報記憶部２１２と部分情報領域２２３に記憶する部分情報ＰＥＣ１［ｉ］を消去する。

Ｓ７０７：記録再生装置１０２は、可搬媒体１０４の部分情報領域２２３に記録する部分情報の次ブロックＰＥＣ１［ｉ］（ｉ＝ｉ＋１）を書込／読出部２１４を介して読み出

す。

【００３７】

（実施の形態２）

図８は、本発明の実施の形態２における、記録再生装置１０２が可搬媒体１０４にコンテンツを移動させる場合の記録再生装置１０２、並びに可搬媒体１０４の機能を示す機能ブロック図である。

記録再生装置１０２は、外部からのコンテンツを受信するコンテンツ受信部２０１と、前記受信したコンテンツを暗号化するために用いる装置記録鍵を記憶する装置記録鍵記憶部２０２と、前記装置記録鍵を用いて、前記受信したコンテンツを暗号化する暗号化部２０３と、前記暗号化したコンテンツを記録する暗号化コンテンツ記録部２０４と、暗号化コンテンツ記録部２０４に記録された前記暗号化したコンテンツを読み出す暗号化コンテンツ読出し部２０５と、前記装置記録鍵を用いて、暗号化コンテンツ読出し部２０５が読み出した前記暗号化したコンテンツを復号する復号部２０６と、復号部２０６が復号したコンテンツを（圧縮）変換する変換部２０７と、変換部２０７が変換したコンテンツを暗号化するために用いる媒体記録鍵を生成する媒体記録鍵生成部２０８と、前記媒体記録鍵を記憶する媒体記録鍵記憶部２０９と、前記媒体記録鍵を用いて、変換部２０７が変換したコンテンツを暗号化する暗号化部２１０と、復号部２０６が復号したコンテンツから部分情報を選択する部分情報選択部２１１と、前記部分情報を記憶する部分情報記憶部２１２と、部分情報記憶部２１２に記憶された前記部分情報に対応して、復号部２０６が復号した前記復号したコンテンツを加工し、暗号化部２０３で前記装置記録鍵を用いて暗号化し、暗号化コンテンツ記録部２０４に書込みを行う部分情報書込部２１３と、媒体記録鍵記憶部２０９に記録された前記媒体記録鍵を用いて前記部分情報を暗号化もしくは復号化を行う暗復号化部８０１と、暗号化部２１０が暗号化したコンテンツ、前記媒体記録鍵、並びに暗復号化部８１０が暗号化した部分情報を可搬媒体１０４に書き込む、あるいは可搬媒体１０４から読み出す書込／読出部２１４とを備える。媒体記録鍵記憶部２０９に記憶する鍵データは、書込／読出部２１４を介して当該鍵データが媒体に書き込まれた後は、そのデータが消去される。

【００３８】

また、可搬媒体１０４は、暗号化コンテンツを記録する暗号化コンテンツ領域２２１と、媒体記録鍵を記録する媒体記録鍵領域２２２と、部分情報を記録する部分情報領域２２３を備える。可搬媒体１０４が備える媒体記録鍵領域２２２は、鍵を記録するための安全な領域であり、例えば、可搬媒体との認証をパスした装置のみがデータの読み書き可能となるような領域である。

【００３９】

図３は暗号化コンテンツ記録部に記録された暗号化コンテンツを示す図である。暗号化コンテンツは１つ以上のブロック（ＥＣ１［1］、ＥＣ１［2］、・・・、ＥＣ１［N］）に分けて記録され、各ブロックは装置記録鍵を用いて暗号化されている。

次に、図４および図９を用いて、記録再生装置１０２から、可搬媒体１０４へコンテンツを移動する場合の動作について説明する。

【００４０】

Ｓ４０１：記録再生装置１０２は、媒体記録鍵生成部２０８において媒体記録鍵Ｋ２を生成して、媒体記録鍵記憶部２０９に、前記生成した媒体記録鍵を記憶する。

Ｓ４０２：記録再生装置１０２は、書込／読出部２１４を介して媒体記録鍵Ｋ２を媒体記録鍵領域２２３に書き出す。

Ｓ４０３：記録再生装置１０２は、暗号化コンテンツ読出し部２０５において暗号化コンテンツ記録部２０４に記録する暗号化コンテンツの先頭ブロックＥＣ１［ｉ］（ｉ＝１）を読み出す。

【００４１】

Ｓ４０４：記録再生装置１０２は、暗号化コンテンツのブロックの読み出しに失敗したらＳ４０６に処理を分岐する。そうでなければ、Ｓ５００に処理を分岐する。

Ｓ５００：読み出した暗号化コンテンツのブロックを可搬媒体に移動する。
Ｓ４０５：記録再生装置１０２は、暗号化コンテンツ読出し部２０５において暗号化コンテンツ記録部２０４に記録する暗号化コンテンツの次ブロックＥＣ１［ｉ］（ｉ＝ｉ＋１）を読み出す。
【００４２】
Ｓ４０６：記録再生装置１０２は、媒体記録鍵記憶部２０９に記録された媒体記録鍵Ｋ２を消去する。
以下のステップは、Ｓ５００を詳細化したものである。
Ｓ９０１：記録再生装置１０２は、暗号化コンテンツの１ブロックＥＣ１［ｉ］を復号部２０６において、装置記録鍵記憶部２０２に記憶する装置記録鍵Ｋ１を用いて復号し、Ｃ１［ｉ］を生成する。
【００４３】
Ｓ９０２：記録再生装置１０２は、変換部２０７において、Ｓ９０１で復号したブロックＣ１［ｉ］を（圧縮）変換し、Ｃ２［ｉ］を生成する。
Ｓ９０３：記録再生装置１０２は、暗号化部２１０において、Ｓ４０１で生成／記憶した媒体記録鍵Ｋ２を用いて、Ｓ９０２で変換したコンテンツＣ２［ｉ］を暗号化し、ＥＣ２［ｉ］を生成する。
【００４４】
Ｓ９０４：記録再生装置１０２は、Ｓ９０３で暗号化したコンテンツＥＣ２［ｉ］を、書込／読出部２１４を介して可搬媒体１０４の暗号化コンテンツ領域２２１へ記録する。
Ｓ９０５：記録再生装置１０２は、部分情報選択部２１１において、Ｓ９０１で復号化したＣ１［ｉ］から、部分情報ＰＣ１［ｉ］を選択（例えば、ブロックの構成を示すタグ情報部分を選択）し、部分情報記憶部２１２へ記録する。
【００４５】
Ｓ９０６：記録再生装置１０２は、Ｓ９０１で復号化したＣ１［ｉ］において部分情報ＰＣ１［ｉ］として選択した部分を無意味な情報（例えば全て０）に変更し、さらに暗号化部２０３で装置記録鍵Ｋ１を暗号化鍵として暗号化したもので、暗号化コンテンツ記録部２０４に記録された暗号化コンテンツの１ブロックＥＣ１［ｉ］に対応する部分を上書きする。
【００４６】
Ｓ９０７：記録再生装置１０２は、部分情報記憶部２１２に記憶する部分情報ＰＣ１［ｉ］を暗復号化部８０１で媒体記録鍵Ｋ２を用いて暗号化してＥＰＣ１［ｉ］とし、書込／読出部２１４を介して可搬媒体１０４の部分情報領域２２３へ記録する。
Ｓ９０８：記録再生装置１０２は装置内の、部分情報記憶部２１２に記憶する部分情報ＰＣ１［ｉ］と、Ｓ９０１で生成したＣ１［ｉ］と、Ｓ９０２で生成したＣ２［ｉ］と、Ｓ９０３で生成したＥＣ２［ｉ］と、Ｓ９０７で生成したＥＰＣ２［ｉ］を消去する。
【００４７】
図１０は、記録再生装置１０２から可搬媒体１０４へのコンテンツの移動が完了したときの、可搬媒体１０４の記録状態を示した図である。
次に、図１１を用いて、可搬媒体１０４から，記録再生装置１０２へコンテンツを移動する場合の動作について説明する。
Ｓ１１０１：記録再生装置１０２は、可搬媒体１０４の装置記録鍵領域２２２に記録する媒体記録鍵Ｋ２を書込／読出部２１４を介して読み出し、媒体記録鍵記憶部２０９に記録する。
【００４８】
Ｓ１１０２：可搬媒体１０４は、暗号化コンテンツ領域２２１に記録する暗号化コンテンツＥＣ２［ｉ］（ｉ＝１～Ｎ）、並びに媒体記録鍵領域２２２に記録する媒体記録鍵Ｋ２を消去する。
Ｓ１１０３：記録再生装置１０２は、暗号化コンテンツ読出し部２０５において暗号化コンテンツ記録部２０４に記録する暗号化コンテンツの先頭ブロックＥＣ１［ｉ］（ｉ＝

１）を暗号化コンテンツ読出し部２０５を介して読出し、さらに可搬媒体１０４の部分情報領域２２３に記録する部分情報の先頭ブロックＥＰＣ１［ｉ］（ｉ＝１）を書込／読出部２１４を介して読み出す。

【００４９】

Ｓ１１０４：記録再生装置１０２は、暗号化コンテンツのブロック及び部分情報のブロックの読み出しに失敗したらＳ１１１０に処理を分岐する。そうでなければ、Ｓ１１０５に処理を分岐する。

Ｓ１１０５：記録再生装置１０２は、暗号化コンテンツの１ブロックＥＣ１［ｉ］を復号部２０６において、装置記録鍵記憶部２０２に記憶する装置記録鍵Ｋ１を用いて復号し、Ｃ１［ｉ］を生成する。

【００５０】

Ｓ１１０６：記録再生装置１０２は、読出した部分情報ＥＰＣ１［ｉ］を暗復号化部８０１において、媒体記録鍵記憶部２０９に記憶する媒体記録鍵Ｋ２を用いて復号し、ＰＣ１［ｉ］として部分情報記憶部２１２へ記録する。

Ｓ１１０７：記録再生装置１０２は、Ｓ１１０５で生成したＣ１［ｉ］に対し、部分情報記憶部２１２へ記録されたＰＣ１［ｉ］の相当する箇所をＰＣ１［ｉ］で上書きし、さらに暗号化部２０３で装置記録鍵Ｋ１を暗号化鍵として暗号化したもので、暗号化コンテンツ記録部２０４に記録された暗号化コンテンツの１ブロックＥＣ１［ｉ］に対応する部分を上書きする。

【００５１】

Ｓ１１０８：記録再生装置１０２は装置内の、部分情報記憶部２１２に記憶する部分情報ＰＣ１［ｉ］と、Ｓ１１０５で生成したＣ１［ｉ］と、さらに部分情報領域２２３の部分情報ＥＰＣ１［ｉ］を消去する。

Ｓ１１０９：記録再生装置１０２は、暗号化コンテンツ読出し部２０５において暗号化コンテンツ記録部２０４に記録する暗号化コンテンツの次ブロックＥＣ１［ｉ］（ｉ＝ｉ＋１）を読出し、さらに可搬媒体１０４の部分情報領域２２３に記録する部分情報の次ブロックＰＥＣ１［ｉ］（ｉ＝ｉ＋１）を書込／読出部２１４を介して読み出す。

【００５２】

Ｓ１１１０：記録再生装置１０２は、媒体記録鍵記憶部２０９に記録された媒体記録鍵Ｋ２を消去する。

（実施の形態３）

図１２は、本発明の実施の形態３における、記録再生装置１０２が可搬媒体１０４にコンテンツを移動させる場合の記録再生装置１０２、並びに可搬媒体１０４の機能を示す機能ブロック図である。

【００５３】

記録再生装置１０２は、外部からのコンテンツを受信するコンテンツ受信部２０１と、前記受信したコンテンツを暗号化するために用いる装置記録鍵を記憶する装置記録鍵記憶部２０２と、前記装置記録鍵を用いて、前記受信したコンテンツを暗号化する暗号化部２０３と、前記暗号化したコンテンツを記録する暗号化コンテンツ記録部２０４と、暗号化コンテンツ記録部２０４に記録された前記暗号化したコンテンツを読み出す暗号化コンテンツ読出し部２０５と、前記装置記録鍵を用いて、暗号化コンテンツ読出し部２０５が読み出した前記暗号化したコンテンツを復号する復号部２０６と、前記復号したコンテンツを（圧縮）変換する変換部２０７と、変換部２０７が変換したコンテンツを暗号化するために用いる媒体記録鍵を生成する媒体記録鍵生成部２０８と、前記媒体記録鍵を記憶する媒体記録鍵記憶部２０９と、前記媒体記録鍵を用いて、変換部２０７が変換したコンテンツを暗号化する暗号化部２１０と、復号部２０６が復号したコンテンツから部分情報として選択する箇所を決定し、暗号化コンテンツ読出し部２０５が読み出した前記暗号化したコンテンツから前記選択箇所の部分情報を抽出する部分情報選択部２１１と、前記部分情報を記憶する部分情報記憶部２１２と、部分情報記憶部２１２に記憶された前記部分情報に対応して暗号化コンテンツ記録部２０４に書込みを行う部分情報書込部２１３と、前記

暗号化したコンテンツ、前記媒体記録鍵、並びに前記部分情報を可搬媒体１０４に書き込む、あるいは可搬媒体１０４から読み出す書込／読出部２１４とを備える。媒体記録鍵記憶部２０９に記憶する鍵データは、書込／読出部２１４を介して当該鍵データが可搬媒体１０４に書き込まれた後は、そのデータが消去される。

【００５４】

また、可搬媒体１０４は、暗号化コンテンツを記録する暗号化コンテンツ領域２２１と、媒体記録鍵を記録する媒体記録鍵領域２２２と、部分情報を記録する部分情報領域２２３を備える。可搬媒体１０４が備える媒体記録鍵領域２２２は、鍵を記録するための安全な領域であり、例えば、可搬媒体との認証をパスした装置のみがデータの読み書き可能となるような領域である。

【００５５】

図３は暗号化コンテンツ記録部に記録された暗号化コンテンツを示す図である。暗号化コンテンツは１つ以上のブロックに（ＥＣ１［1］、ＥＣ１［2］、・・・、ＥＣ１［Ｎ］）分けて記録され、各ブロックは装置記録鍵を用いて暗号化されている。

次に、図４および図１３を用いて、記録再生装置１０２から、可搬媒体１０４へコンテンツを移動する場合の動作について説明する。

【００５６】

Ｓ４０１：記録再生装置１０２は、媒体記録鍵生成部２０８において媒体記録鍵Ｋ２を生成して、媒体記録鍵記憶部２０９に、前記生成した媒体記録鍵を記憶する。

Ｓ４０２：記録再生装置１０２は、書込／読出部２１４において媒体記録鍵Ｋ２を媒体記録鍵領域２２２に書き出す。

Ｓ４０３：記録再生装置１０２は、暗号化コンテンツ読出し部２０５において暗号化コンテンツ記録部２０４に記録する暗号化コンテンツの先頭ブロックＥＣ１［ｉ］（ｉ＝１）を読み出す。

【００５７】

Ｓ４０４：記録再生装置１０２は、暗号化コンテンツのブロックの読み出しに失敗したらＳ４０６に処理を分岐する。そうでなければ、Ｓ５００に処理を分岐する。

Ｓ５００：読み出した暗号化コンテンツのブロックを可搬媒体に移動する。

Ｓ４０５：記録再生装置１０２は、暗号化コンテンツ読出し部２０５において暗号化コンテンツ記録部２０４に記録する暗号化コンテンツの次ブロックＥＣ１［ｉ］（ｉ＝ｉ＋１）を読み出す。

【００５８】

Ｓ４０６：記録再生装置１０２は、媒体記録鍵記憶部２０９に記録された媒体記録鍵Ｋ２を消去する。

以下のステップは、Ｓ５００を詳細化したものである。

Ｓ１３０１：記録再生装置１０２は、暗号化コンテンツの１ブロックＥＣ１［ｉ］を復号部２０６において、装置記録鍵記憶部２０２に記憶する装置記録鍵Ｋ１を用いて復号し、Ｃ１［ｉ］を生成する。

【００５９】

Ｓ１３０２：記録再生装置１０２は、変換部２０７において、Ｓ１３０１で復号したブロックＣ１［ｉ］を（圧縮）変換し、Ｃ２［ｉ］を生成する。

Ｓ１３０３：記録再生装置１０２は、暗号化部２１０において、Ｓ４０１で生成／記憶した媒体記録鍵Ｋ２を用いて、Ｓ１３０２で変換したコンテンツＣ２［ｉ］を暗号化し、ＥＣ２［ｉ］を生成する。

【００６０】

Ｓ１３０４：記録再生装置１０２は、Ｓ１３０３で暗号化したコンテンツＥＣ２［ｉ］を、書込／読出部２１４を介して可搬媒体１０４の暗号化コンテンツ領域２２１へ記録する。

Ｓ１３０５：記録再生装置１０２は、部分情報選択部２１１において、暗号化コンテンツの１ブロックＥＣ１［ｉ］から部分情報として選択する箇所を決定し、暗号化コンテン

ツＥＣｌ［ｉ］の該当箇所から部分情報ＰＥＣｌ［ｉ］を選択（例えば、ブロックの先頭から６４ｂｙｔｅと５１２ｂｙｔｅ目から６４ｂｙｔｅなどのように選択）し、位置情報と共に部分情報記憶部２１２へ記録する。

【００６１】

Ｓ１３０６：記録再生装置１０２は、暗号化コンテンツ記録部２０４に記録された暗号化コンテンツの、部分情報記憶部２１２へ記録されたＰＥＣｌ［ｉ］に対応する部分を無意味な情報（例えば全て０）で上書きする。

Ｓ１３０７：記録再生装置１０２は、部分情報記憶部２１２に記憶する部分情報ＰＥＣｌ［ｉ］を、書込／読出部２１４を介して可搬媒体１０４の部分情報領域２２３へ位置情報と共に記録する。

【００６２】

Ｓ１３０８：記録再生装置１０２は装置内の、部分情報記憶部２１２に記憶する部分情報ＰＥＣｌ［ｉ］と、Ｓ１３０１で生成したＣｌ［ｉ］と、Ｓ１３０２で生成したＣ２［ｉ］と、Ｓ１３０３で生成したＥＣ２［ｉ］を消去する。

図６は、記録再生装置１０２から可搬媒体１０４へのコンテンツの移動が完了したときの、可搬媒体１０４の記録状態を示した図である。

【００６３】

次に、図７を用いて、可搬媒体１０４から、記録再生装置１０２へコンテンツを移動する場合の動作について説明する。

Ｓ７０１：可搬媒体１０４は、暗号化コンテンツ領域２２１に記録する暗号化コンテンツＥＣ２［ｉ］（ｉ＝１～Ｎ）、並びに媒体記録鍵領域２２２に記録する媒体記録鍵Ｋ２を消去する。

【００６４】

Ｓ７０２：記録再生装置１０２は、可搬媒体１０４の装置記録鍵領域２２３に記録する部分情報の先頭ブロックＰＥＣｌ［ｉ］（ｉ＝１）を書込／読出部２１４を介して位置情報と共に読み出す。

Ｓ７０３：記録再生装置１０２は、部分情報のブロックの読み出しに失敗したら処理を終了する。そうでなければ、Ｓ７０４に処理を分岐する。

【００６５】

Ｓ７０４：記録再生装置１０２は、読出した部分情報ＰＥＣｌ［ｉ］を部分情報記憶部２１２へ記録する。

Ｓ７０５：記録再生装置１０２は、部分情報記憶部２１２へ記録されたＰＥＣｌ［ｉ］を、暗号化コンテンツ記録部２０４に記録された暗号化コンテンツの対応する部分へ上書きする。

【００６６】

Ｓ７０６：記録再生装置１０２は、部分情報記憶部２１２と部分情報領域２２３に記憶する部分情報ＰＥＣｌ［ｉ］を消去する。

Ｓ７０７：記録再生装置１０２は、可搬媒体１０４の部分情報領域２２３に記録する部分情報の次ブロックＰＥＣｌ［ｉ］（ｉ＝ｉ＋１）を書込／読出部２１４を介して読み出す。

【００６７】

（その他の変形例）

（１）本発明の実施の形態では、記録再生装置から可搬媒体へコンテンツを移動する、あるいは可搬媒体から記録再生装置へコンテンツを移動する構成としたが、本発明はその構成に限定されるものではない。例えば、記録再生装置から、別の記録再生装置へコンテンツを移動する構成であってもよい。

【００６８】

（２）本発明の実施の形態では、可搬媒体から記録再生装置へコンテンツを移動する際、可搬媒体に記録する各種データを消去する構成としたが、本発明はその構成に限定されるものではない。例えば、可搬媒体に記録する暗号化コンテンツは消去せずに、復号に必

要な鍵だけを消去して、前記暗号化コンテンツを利用不可状態にする構成であってもよい。また、データの消去ではなく、データの一部を破壊して利用できない状態にする構成であってもよい。

【００６９】

（３）本発明の実施の形態において、記録再生装置が、コンテンツの移動処理における状態遷移を記憶する記憶部を備える構成であってもよい。記録再生装置は、コンテンツの移動が正しく完了しなかった場合、前記記憶部に記憶する状態遷移に基づいて、コンテンツの移動処理を続けて行うか、コンテンツの移動処理を最初からやり直すかを判断する構成であってもよい。さらに、記録再生装置は、前記記憶部に記憶する状態遷移を利用者に通知する通知部を備える構成であってもよい。その場合、正しく完了しなかった旨を利用者に通知して、利用者からの指示に基づいて、コンテンツの移動処理を続けるか、あるいはコンテンツの移動処理を最初かやり直すかを決定する構成であってもよい。

【００７０】

（４）本発明の実施の形態において、記録再生装置、並びに可搬媒体が、鍵を移動後に消去する場合、鍵の受信側が、鍵の送信側に対して正しく受信できたことを通知して、送信側は前記通知に基づいて受信を確認した後に、鍵を消去する構成であってもよい。

（５）本発明の実施の形態において、コンテンツには当該コンテンツを一意に識別するための識別子が付与されており、可搬媒体に移動させたコンテンツを元の記録再生装置に戻す場合、前記記録再生装置は、自身が保持する暗号化コンテンツの識別子、並びに可搬媒体に記録する暗号化コンテンツの識別子が一致するか否かを判定して、一致した場合に限り、コンテンツを記録再生装置に移動させることを許可する構成であってもよい。また、コンテンツには、コンテンツを一意に識別する識別子の代わりに、移動元の記録再生装置を一意に識別する識別子が付与されている構成であってもよい。この場合、記録再生装置は、コンテンツに付与されている記録再生装置の識別子と、自身の識別子が一致するか否かを判定して、一致した場合に限り、コンテンツを記録再生装置に移動させることを許可する構成であってもよい。

【００７１】

（６）本発明の実施の形態２では、部分情報を媒体記録鍵で暗号化して可搬媒体に記録する構成としたが、本発明はその構成に限定されるものではない。装置固有鍵で暗号化して記録する構成であってもよいし、別の鍵を新たに生成して暗号化して記録する構成であってもよい。

（７）本発明の実施の形態では、コンテンツは外部のコンテンツ供給装置により供給される構成としたが、本発明はその構成に限定されるものではない。例えば、記録再生装置に挿入された記録媒体からコンテンツを読み出す構成であってもよい。

【産業上の利用可能性】

【００７２】

本発明にかかる著作権保護システムは、コンテンツの移動元の記録再生装置が、コンテンツの移動時に当該コンテンツの部分情報も合わせて移動させることにより、記録再生装置内のコンテンツの全てを消去することなく利用不可状態にすることで、移動したコンテンツを再び当該記録再生装置へ戻す場合に、前記部分情報を元に戻す（移動させる）ことにより、元々の高画質コンテンツを復元可能（利用可能）にできるという効果を有し、ユーザ利便性を損なわない著作権保護システムの実現において有用である。

【図面の簡単な説明】

【００７３】

【図１】本発明に係る著作権保護システムの全体構成を示すブロック図

【図２】本発明の第１の実施の形態における機能ブロック図

【図３】本発明の第１、第２及び第３の実施の形態における暗号化コンテンツ記録部に記録された暗号化コンテンツを示す図

【図４】本発明の第１、第２及び第３の実施の形態における記録再生装置から可搬媒体へコンテンツを移動させる際の動作のメインフロー

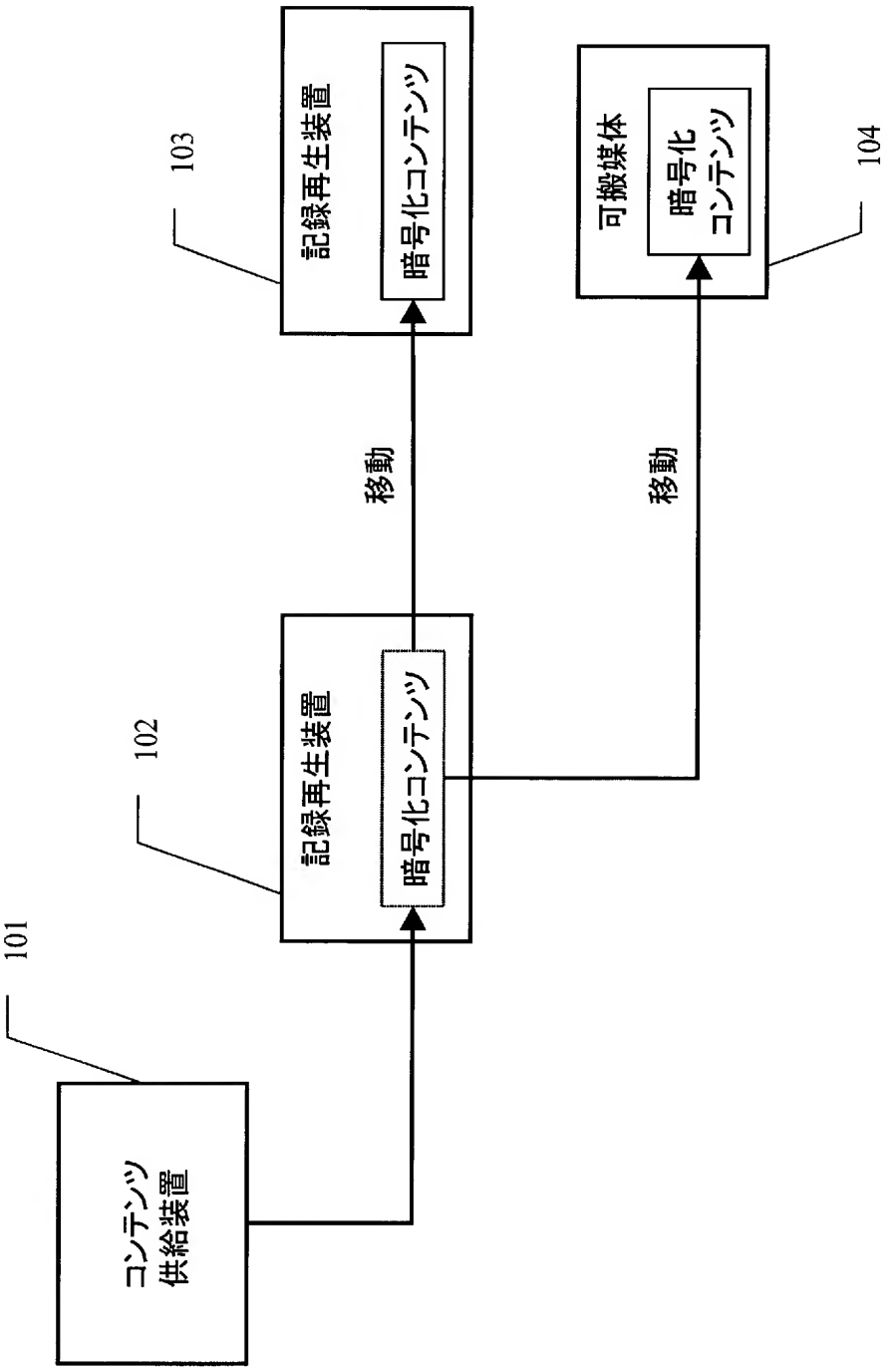
【図５】本発明の第１の実施の形態における記録再生装置から可搬媒体へコンテンツを移動させる際の動作のサブルーチン
【図６】本発明の第１及び第３の実施の形態における部分情報領域に記録された部分情報を示す図
【図７】本発明の第１及び第３の実施の形態における可搬媒体から記録再生装置へコンテンツを移動させる際の動作フロー
【図８】本発明の第２の実施の形態における機能ブロック図
【図９】本発明の第２の実施の形態における記録再生装置から可搬媒体へコンテンツを移動させる際の動作のサブルーチン
【図１０】本発明の第２の実施の形態における部分情報領域に記録された部分情報を示す図
【図１１】本発明の第２の実施の形態における可搬媒体から記録再生装置へコンテンツを移動させる際の動作フロー
【図１２】本発明の第３の実施の形態における機能ブロック図
【図１３】本発明の第３の実施の形態における記録再生装置から可搬媒体へコンテンツを移動させる際の動作のサブルーチン

【符号の説明】

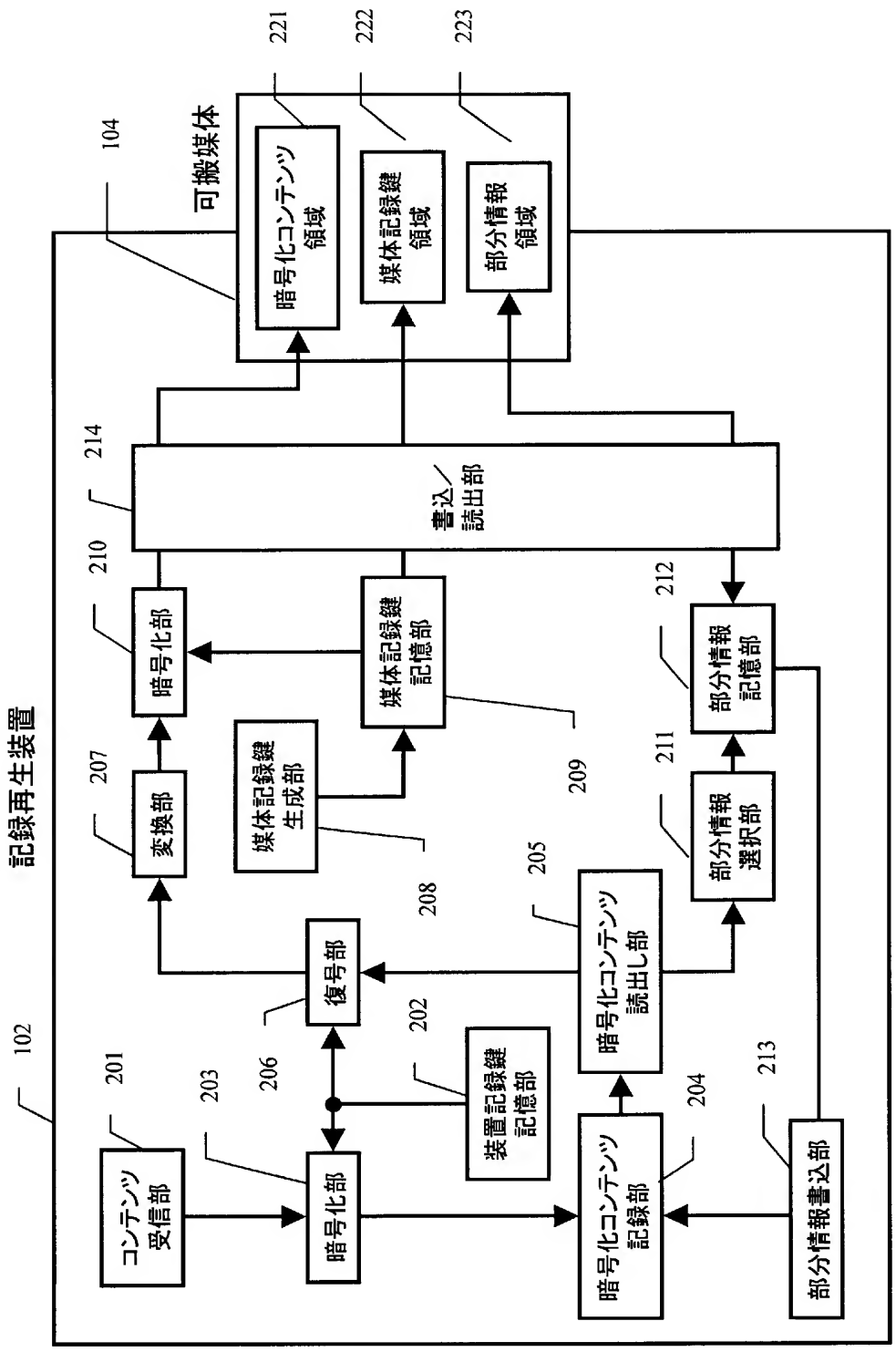
【００７４】

１０１　コンテンツ供給装置
１０２　記録再生装置
１０３　記録再生装置
１０４　可搬媒体
２０１　コンテンツ受信部
２０２　装置記録鍵記憶部
２０３、２１０　暗号化部
２０４　暗号化コンテンツ記録部
２０５　暗号化コンテンツ読出し部
２０６　復号部
２０７　変換部
２０８　媒体記録鍵生成部
２０９　媒体記録鍵記憶部
２１１　部分情報選択部
２１２　部分情報記憶部
２１３　部分情報書込部
２１４　書込読出部
８０１　暗復号化部

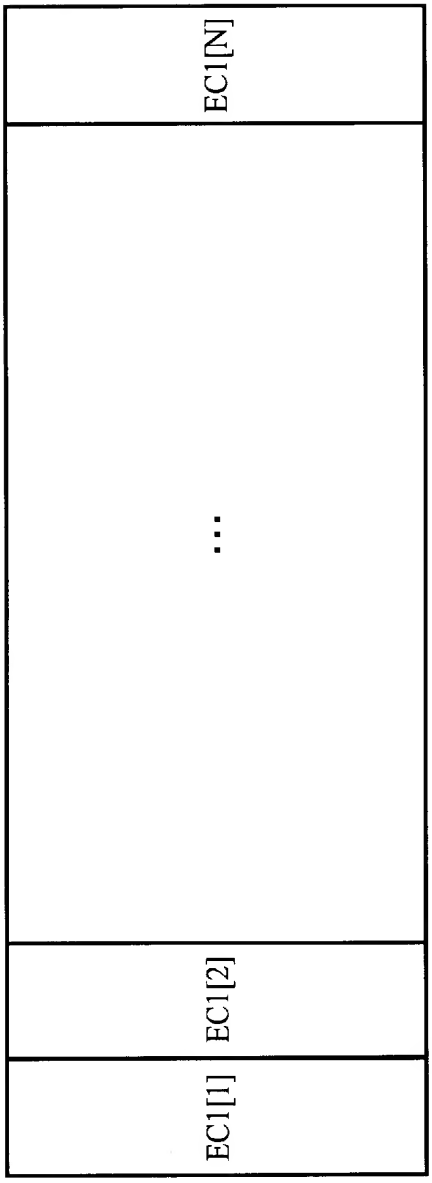
【書類名】図面
【図１】


101
コンテンツ
供給装置
102
記録再生装置
暗号化コンテンツ
移動
103
記録再生装置
暗号化コンテンツ
移動
104
可搬媒体
暗号化
コンテンツ

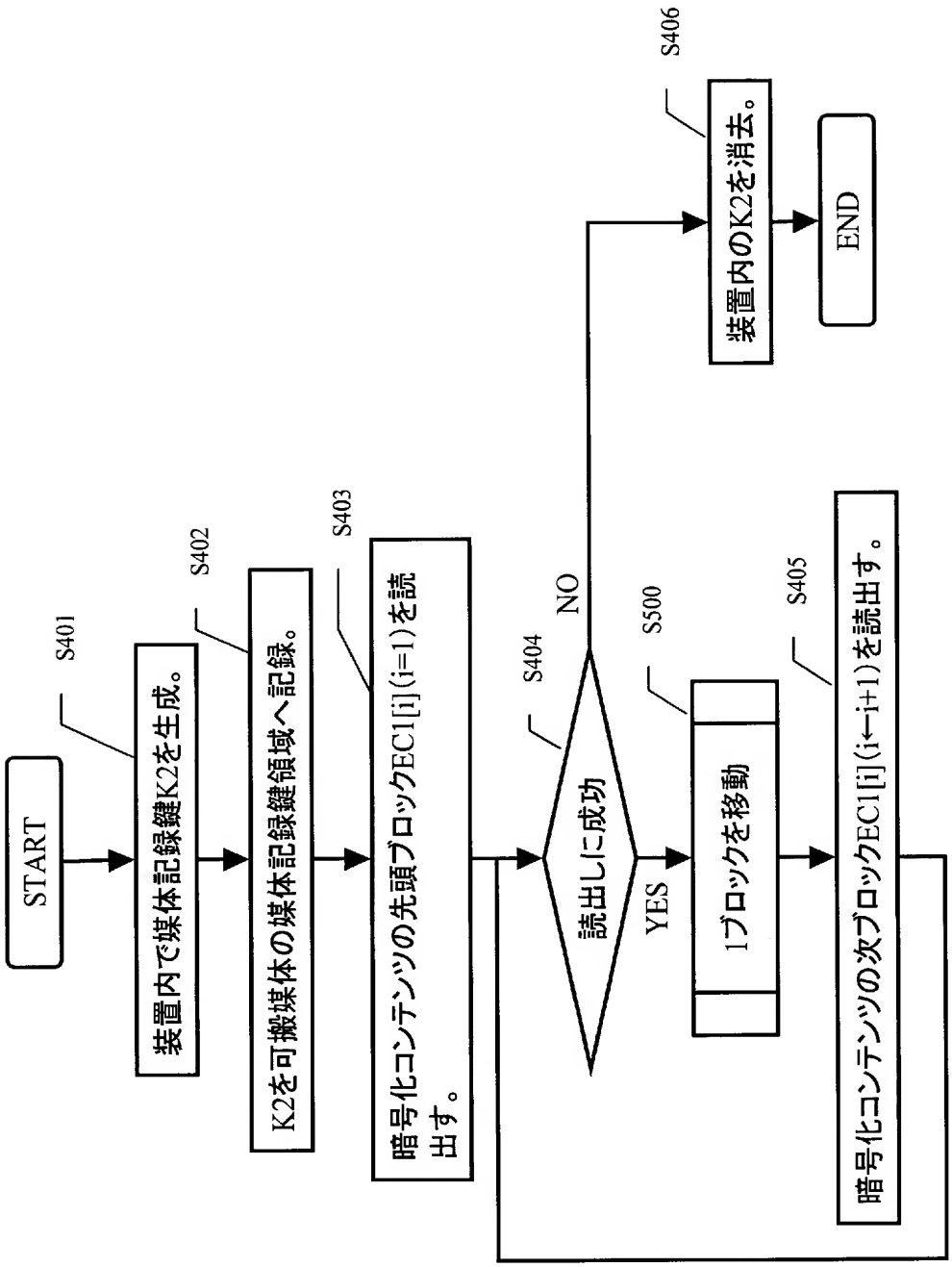
【図２】


記録再生装置
102
104
可搬媒体
221
222
223
暗号化コンテンツ領域
媒体記録鍵領域
部分情報領域
214
書込・読出部
210
暗号化部
媒体記録鍵記憶部
212
部分情報記憶部
207
変換部
媒体記録鍵生成部
209
211
部分情報選択部
208
205
暗号化コンテンツ読出し部
復号部
202
装置記録鍵記憶部
201
203
206
204
213
コンテンツ受信部
暗号化部
暗号化コンテンツ記録部
部分情報書込部

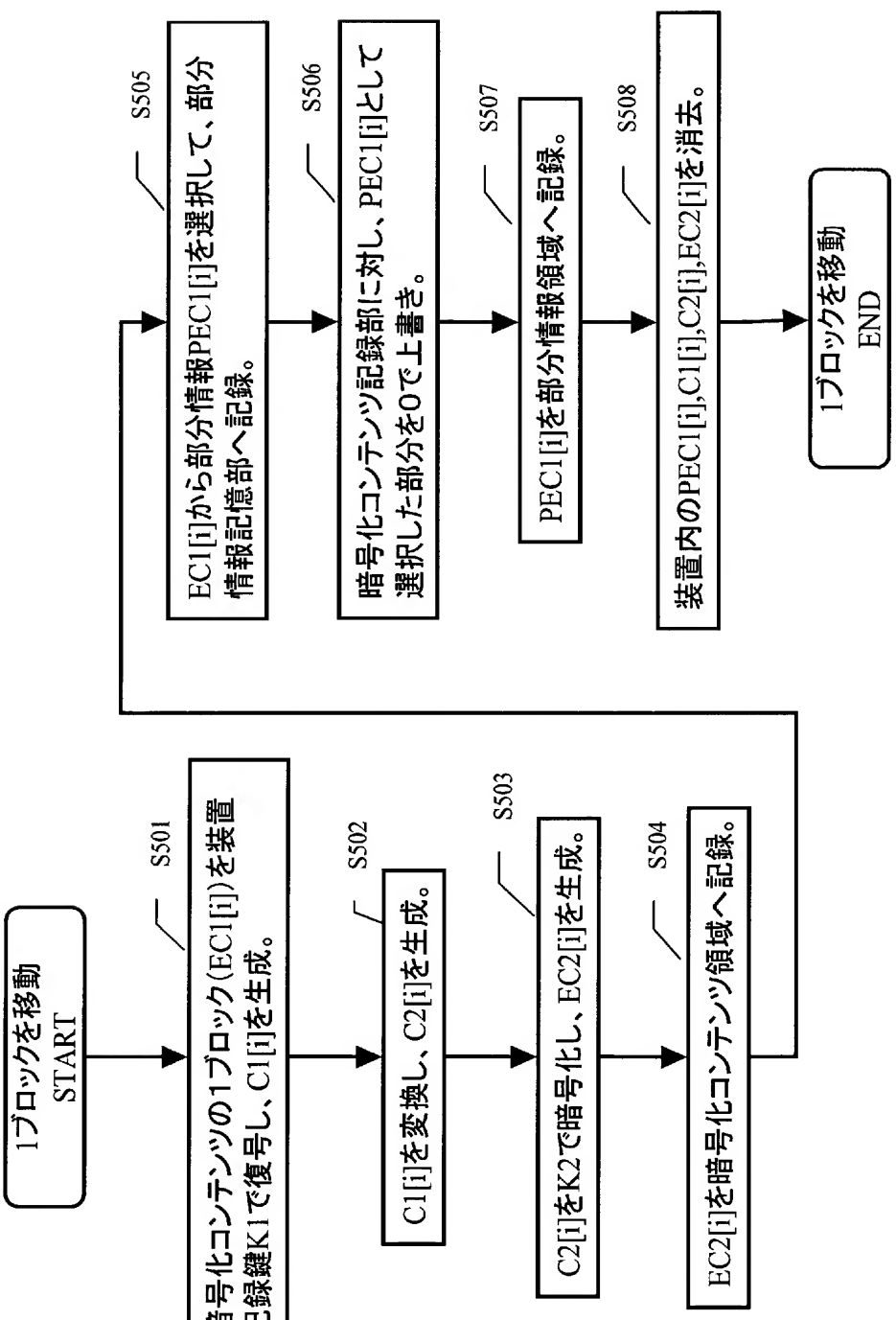
【図３】



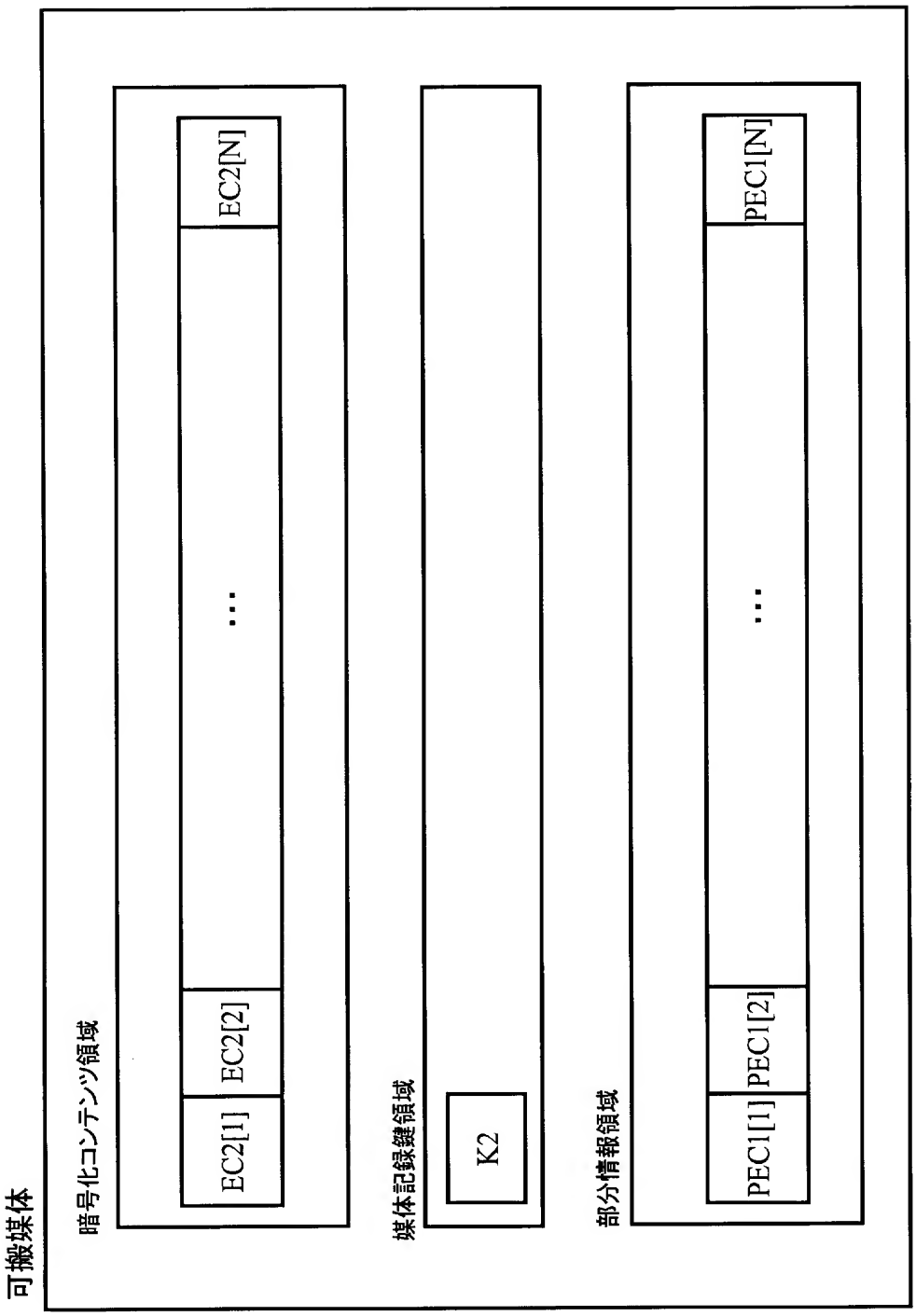
【図４】


START
S401
装置内で媒体記録鍵K2を生成。
S402
K2を可搬媒体の媒体記録鍵領域へ記録。
S403
暗号化コンテンツの先頭ブロックEC1[i](i=1)を読出す。
S404
読出しに成功
NO
YES
S500
1ブロックを移動
S405
暗号化コンテンツの次ブロックEC1[i](i←i+1)を読出す。
S406
装置内のK2を消去。
END

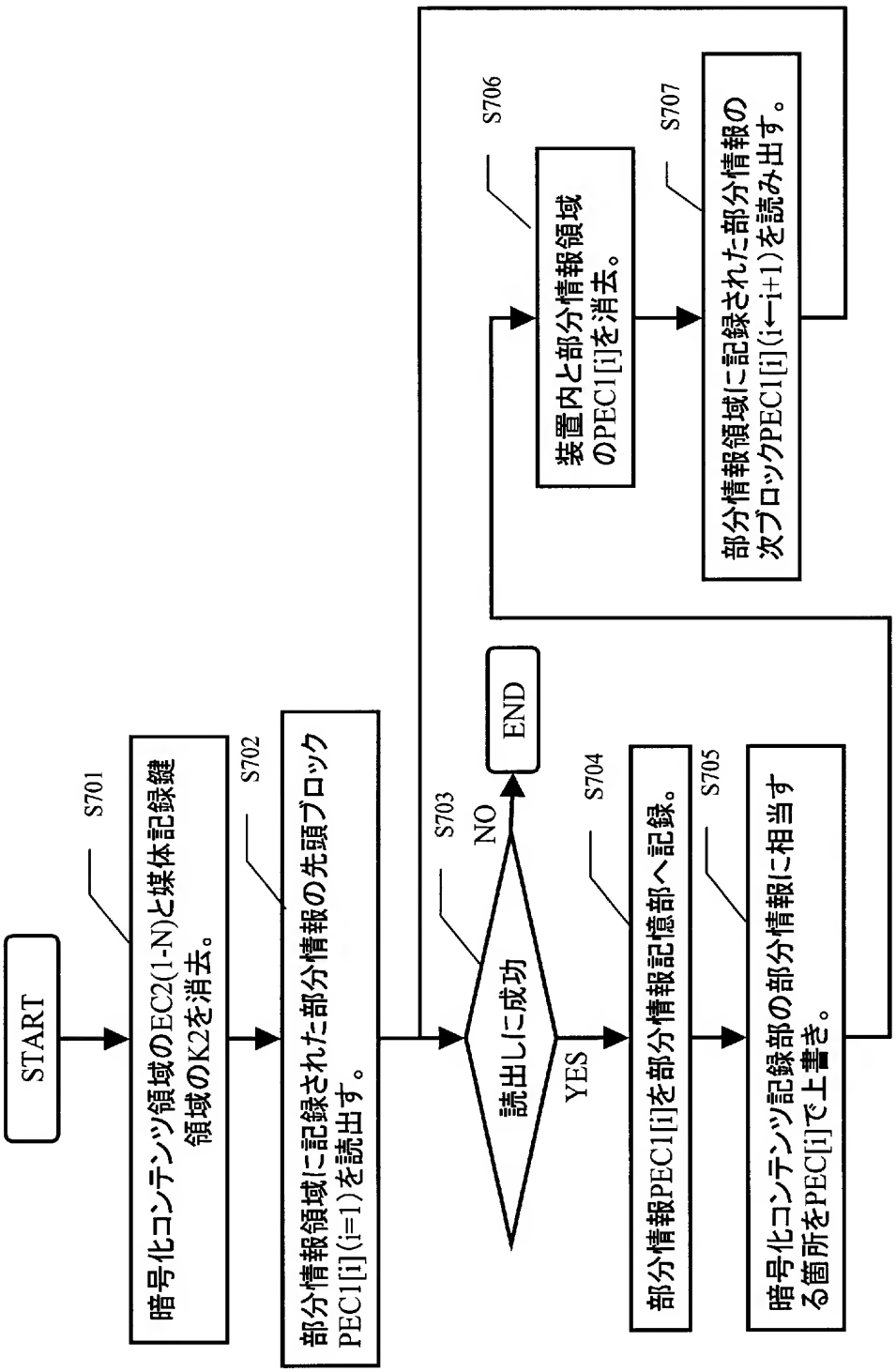
【図５】


1ブロックを移動
START
S501
暗号化コンテンツの1ブロック(EC1[i])を装置記録鍵K1で復号し、C1[i]を生成。
S502
C1[i]を変換し、C2[i]を生成。
S503
C2[i]をK2で暗号化し、EC2[i]を生成。
S504
EC2[i]を暗号化コンテンツ領域へ記録。
S505
EC1[i]から部分情報PEC1[i]を選択して、部分情報記憶部へ記録。
S506
暗号化コンテンツ記録部に対し、PEC1[i]として選択した部分を0で上書き。
S507
PEC1[i]を部分情報領域へ記録。
S508
装置内のPEC1[i],C1[i],C2[i],EC2[i]を消去。
1ブロックを移動
END

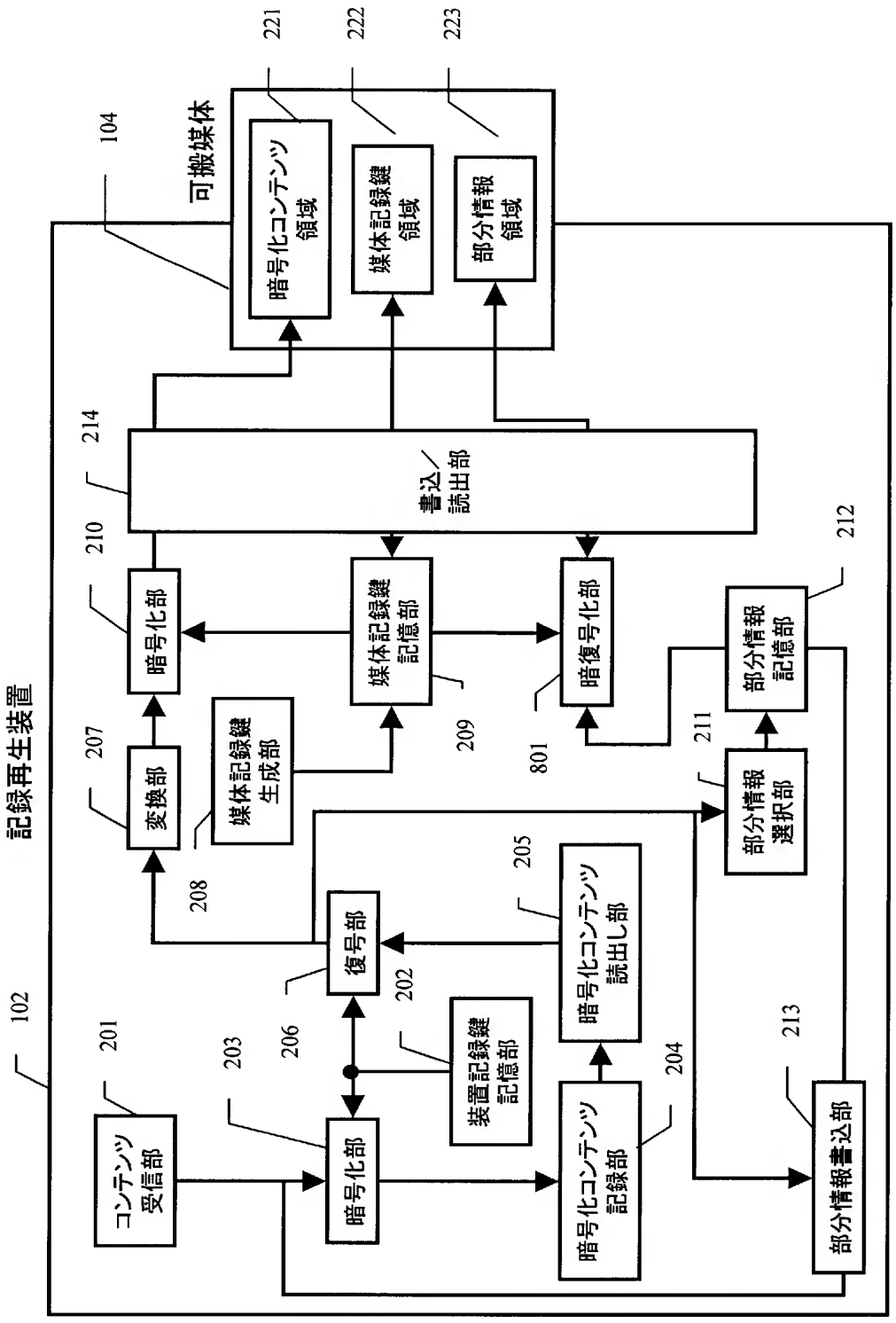
【図６】


可搬媒体
暗号化コンテンツ領域
EC2[1]
EC2[2]
...
EC2[N]
媒体記録鍵領域
K2
部分情報領域
PEC1[1]
PEC1[2]
...
PEC1[N]

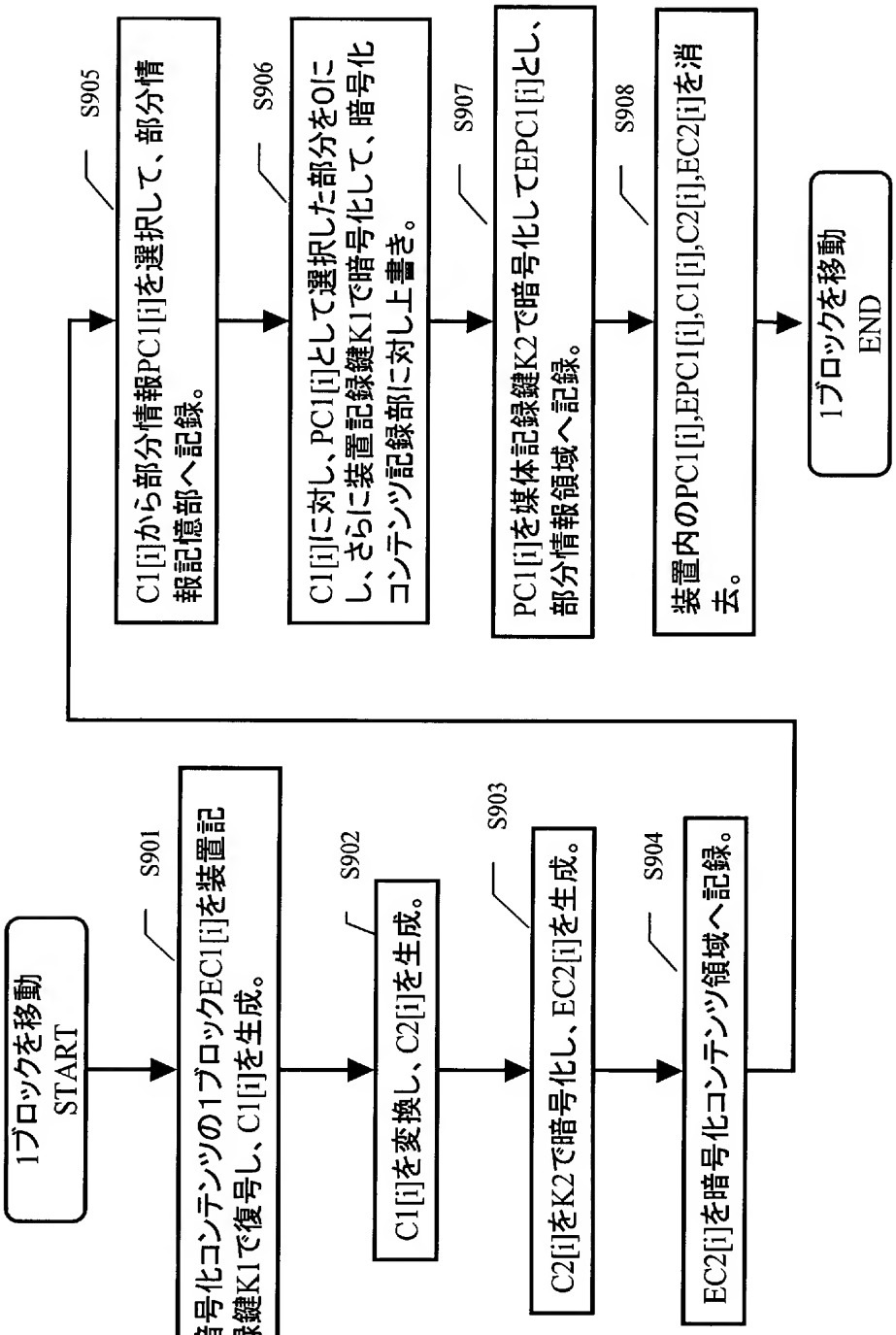
【図７】


START
S701
暗号化コンテンツ領域のEC2(1-N)と媒体記録鍵領域のK2を消去。
S702
部分情報領域に記録された部分情報の先頭ブロックPEC1[i](i=1)を読出す。
S703
読出しに成功
NO
END
YES
S704
部分情報PEC1[i]を部分情報記憶部へ記録。
S705
暗号化コンテンツ記録部の部分情報に相当する箇所をPEC[i]で上書き。
S706
装置内と部分情報領域のPEC1[i]を消去。
S707
部分情報領域に記録された部分情報の次ブロックPEC1[i](i←i+1)を読み出す。

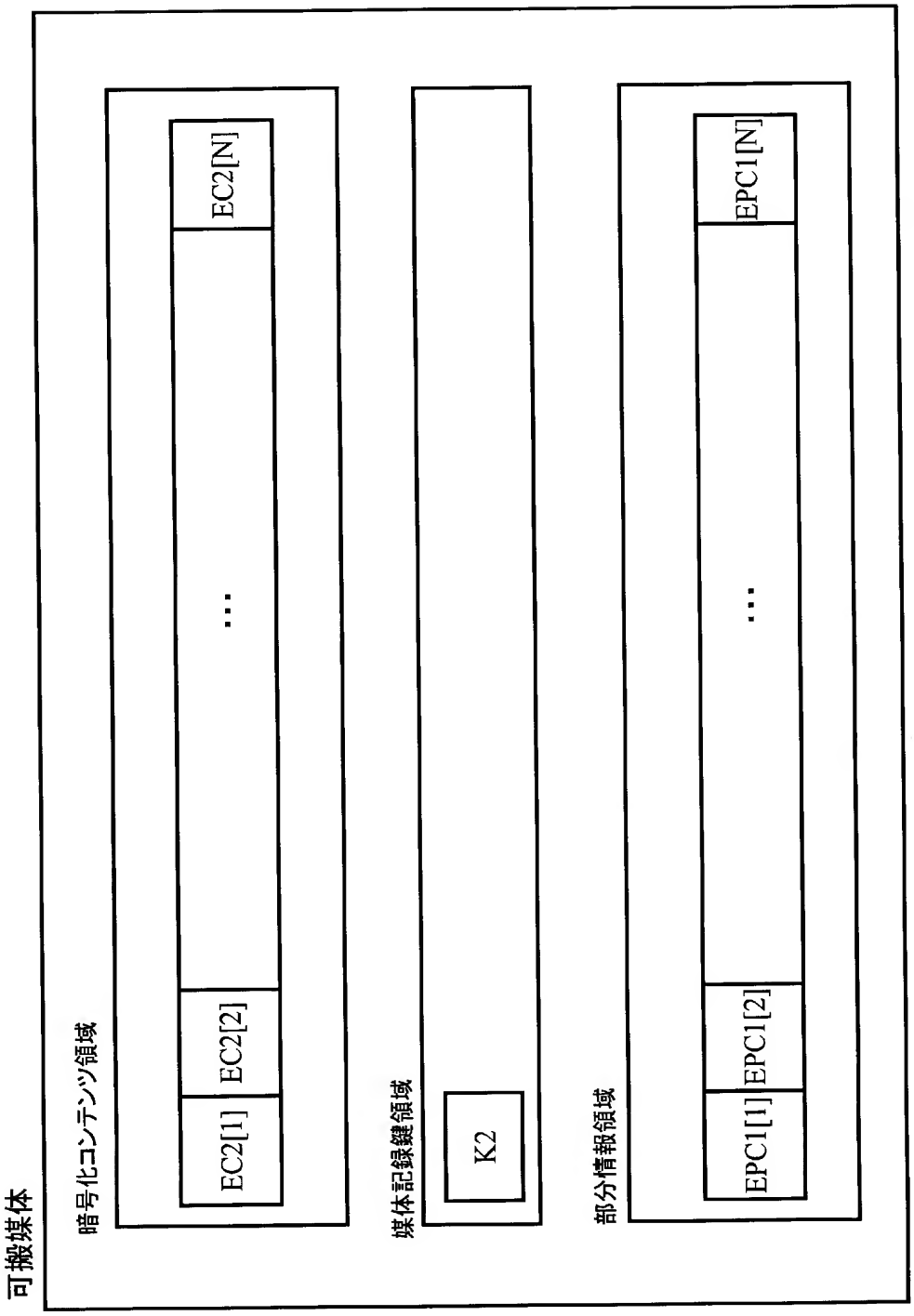
【図８】


記録再生装置
102
104
可搬媒体
221
222
223
暗号化コンテンツ領域
媒体記録鍵領域
部分情報領域
214
書込／読出部
210
暗号化部
媒体記録鍵記憶部
暗復号化部
212
部分情報記憶部
207
変換部
媒体記録鍵生成部
209
801
211
部分情報選択部
208
205
暗号化コンテンツ読出し部
復号部
202
206
201
203
装置記録鍵記憶部
213
コンテンツ受信部
暗号化部
暗号化コンテンツ記録部
204
部分情報書込部

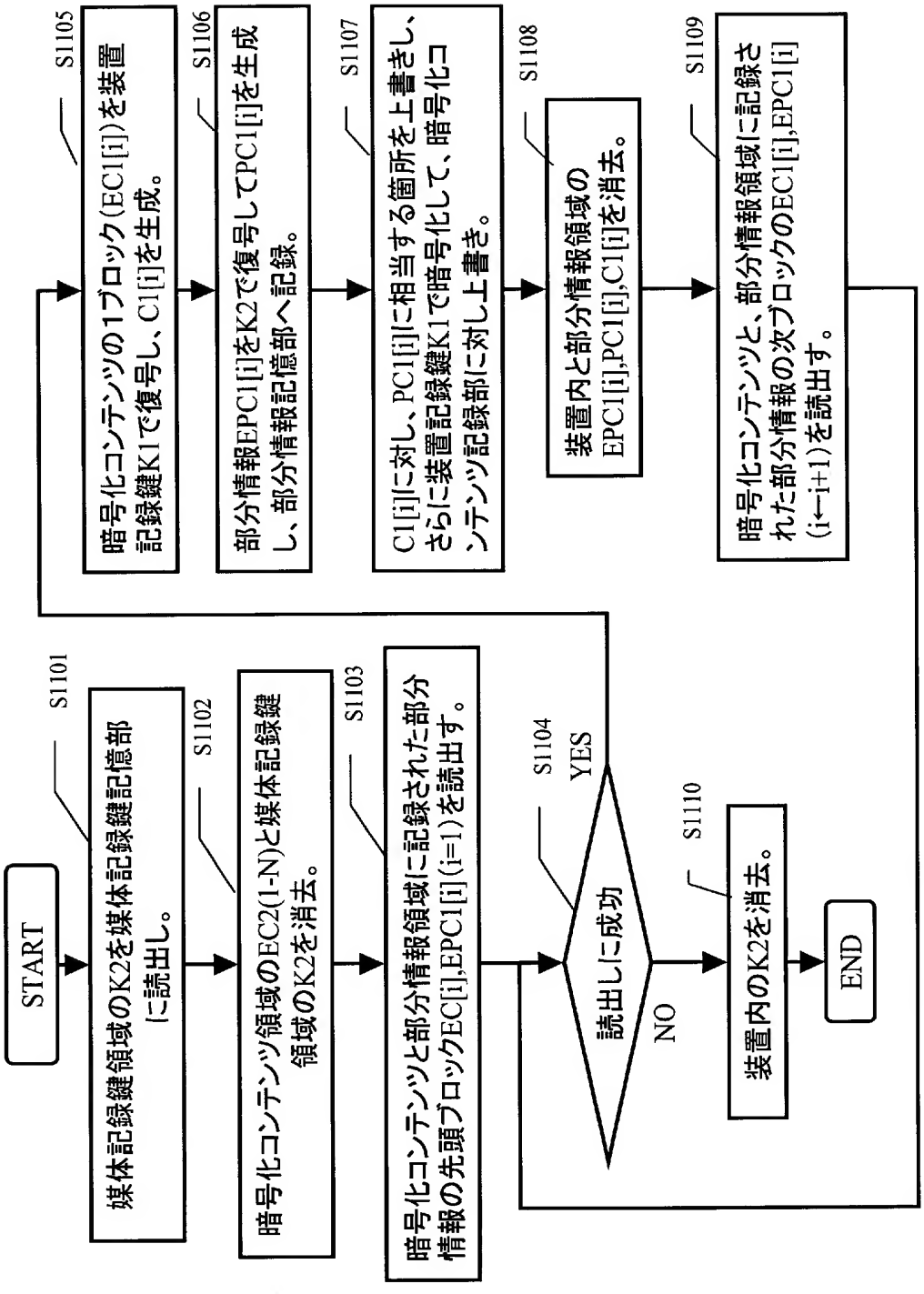
【図９】


1ブロックを移動
START
S901
暗号化コンテンツの1ブロックEC1[i]を装置記録鍵K1で復号し、C1[i]を生成。
S902
C1[i]を変換し、C2[i]を生成。
S903
C2[i]をK2で暗号化し、EC2[i]を生成。
S904
EC2[i]を暗号化コンテンツ領域へ記録。
S905
C1[i]から部分情報PC1[i]を選択して、部分情報記憶部へ記録。
S906
C1[i]に対し、PC1[i]として選択した部分を0にし、さらに装置記録鍵K1で暗号化して、暗号化コンテンツ記録部に対し上書き。
S907
PC1[i]を媒体記録鍵K2で暗号化してEPC1[i]とし、部分情報領域へ記録。
S908
装置内のPC1[i],EPC1[i],C1[i],C2[i],EC2[i]を消去。
1ブロックを移動
END

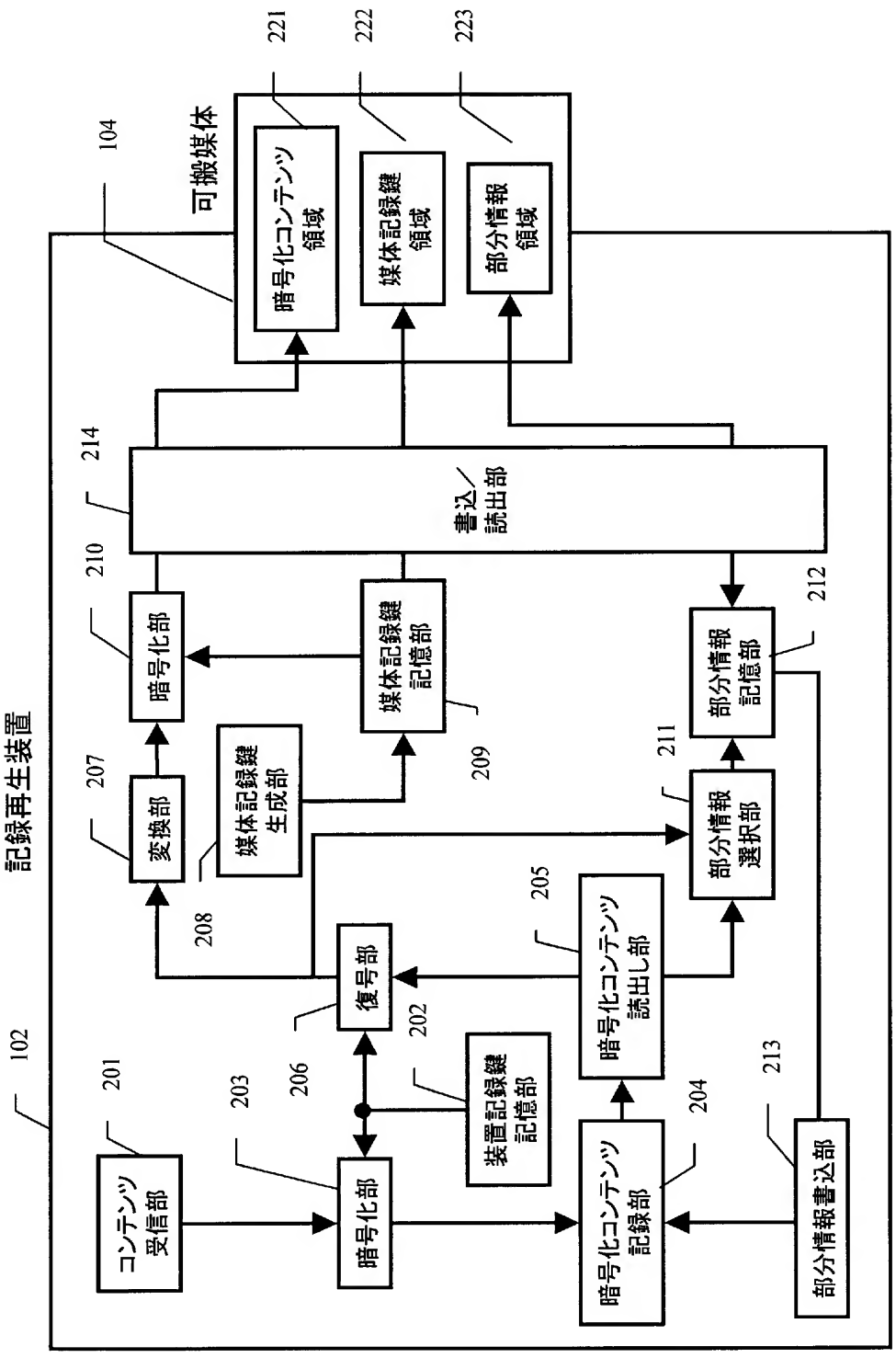
【図１０】


可搬媒体
暗号化コンテンツ領域
EC2[1]
EC2[2]
...
EC2[N]
媒体記録鍵領域
K2
部分情報領域
EPC1[1]
EPC1[2]
...
EPC1[N]

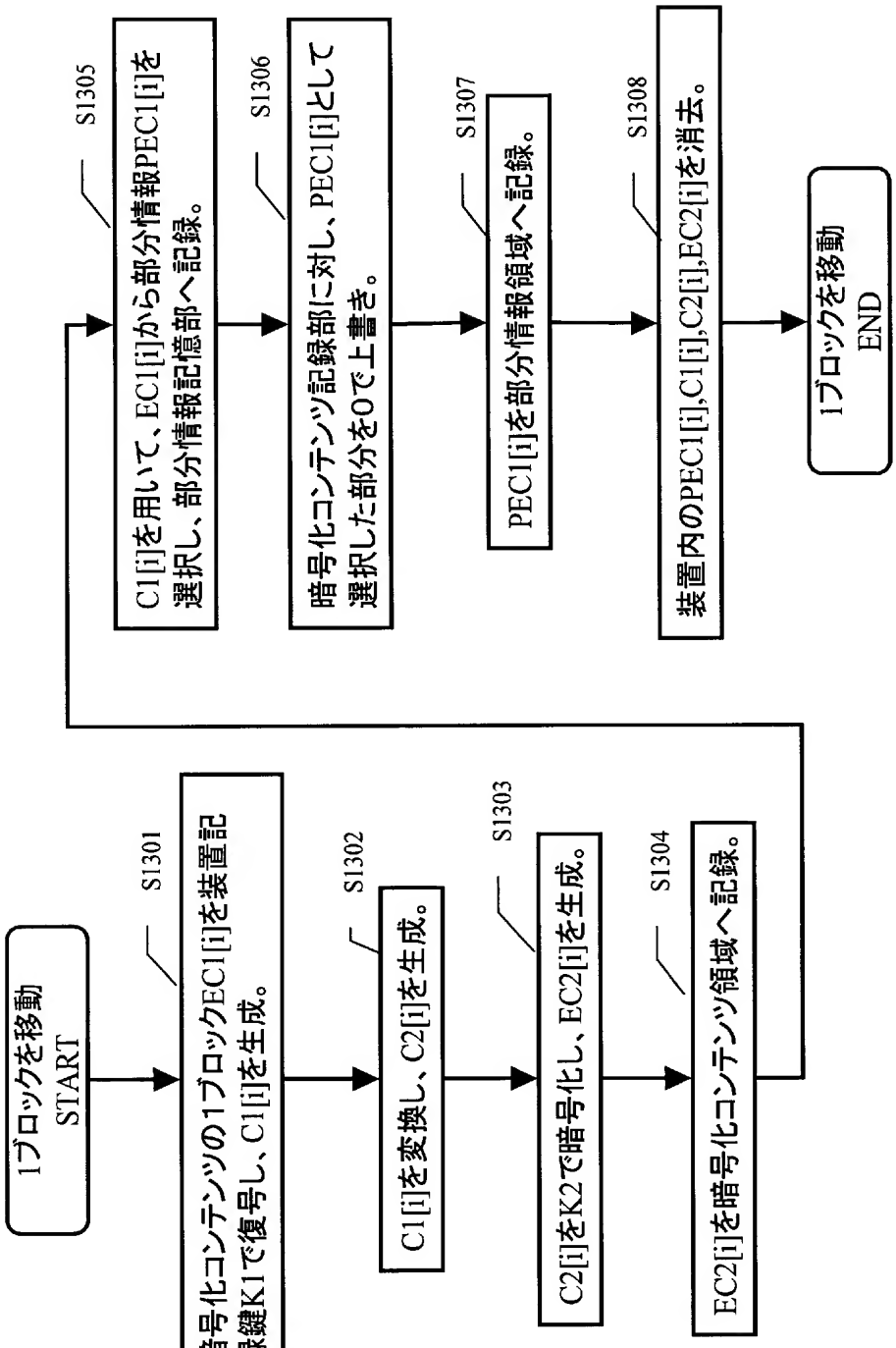
【図１１】


START
S1101
媒体記録鍵領域のK2を媒体記録鍵記憶部に読出し。
S1102
暗号化コンテンツ領域のEC2(1-N)と媒体記録鍵領域のK2を消去。
S1103
暗号化コンテンツと部分情報領域に記録された部分情報の先頭ブロックEC[i],EPC1[i](i=1)を読出す。
S1104
読出しに成功
YES
NO
S1105
暗号化コンテンツの1ブロック(EC1[i])を装置記録鍵K1で復号し、C1[i]を生成。
S1106
部分情報EPC1[i]をK2で復号してPC1[i]を生成し、部分情報記憶部へ記録。
S1107
C1[i]に対し、PC1[i]に相当する箇所を上書きし、さらに装置記録鍵K1で暗号化して、暗号化コンテンツ記録部に対し上書き。
S1108
装置内と部分情報領域のEPC1[i],PC1[i],C1[i]を消去。
S1109
暗号化コンテンツと、部分情報領域に記録された部分情報の次ブロックのEC1[i],EPC1[i](i←i+1)を読出す。
S1110
装置内のK2を消去。
END

【図１２】


記録再生装置
102
104
可搬媒体
221
222
223
暗号化コンテンツ領域
媒体記録鍵領域
部分情報領域
214
書込／読出部
210
暗号化部
媒体記録鍵記憶部
209
212
部分情報記憶部
207
変換部
媒体記録鍵生成部
208
211
部分情報選択部
205
暗号化コンテンツ読出し部
復号部
202
206
装置記録鍵記憶部
201
コンテンツ受信部
203
暗号化部
204
暗号化コンテンツ記録部
213
部分情報書込部

【図１３】


1ブロックを移動
START
S1301
暗号化コンテンツの1ブロックEC1[i]を装置記録鍵K1で復号し、C1[i]を生成。
S1302
C1[i]を変換し、C2[i]を生成。
S1303
C2[i]をK2で暗号化し、EC2[i]を生成。
S1304
EC2[i]を暗号化コンテンツ領域へ記録。
S1305
C1[i]を用いて、EC1[i]から部分情報PEC1[i]を選択し、部分情報記憶部へ記録。
S1306
暗号化コンテンツ記録部に対し、PEC1[i]として選択した部分を0で上書き。
S1307
PEC1[i]を部分情報領域へ記録。
S1308
装置内のPEC1[i],C1[i],C2[i],EC2[i]を消去。
1ブロックを移動
END

【書類名】要約書
【要約】
【課題】　移動元のコンテンツが高画質コンテンツであり、その画質を劣化させるなどしてサイズを小さく圧縮変換してからコンテンツの移動を行った場合、圧縮変換されたコンテンツだけがユーザの下に残り、高画質コンテンツが失われてしまう。
【解決手段】　コンテンツの移動時に当該コンテンツの部分情報を移動させることにより、記録再生装置内のコンテンツの全てを消去せずに利用不可状態にすることで、移動したコンテンツを再び戻す場合に、前記部分情報を移動させることにより、元々の高画質コンテンツを利用可能にする。
【選択図】　図１

出願人履歴

０００００５８２１
19900828
新規登録

大阪府門真市大字門真１００６番地
松下電器産業株式会社